FREECOM

MANUAL

STORAGE GATEWAY

NETWORK HARD DRIVE / 3.5" / STORAGE SERVER
BACKUP SERVER / EMAIL SERVER / ROUTER / AND MORE

STORAGE GATEWAY WLAN

NETWORK HARD DRIVE / 3.5" / STORAGE SERVER
BACKUP SERVER / EMAIL SERVER / ROUTER / AND MORE

Rev. 618

Congratulations

Congratulations on your purchase of the Freecom™ Storage Gateway (FSG). The FSG provides central network storage or Network Attached Storage (NAS) and a secure connection for multiple personal computers (PCs) to the Internet through an external modem.

If you are unfamiliar with networking and routing basics, refer to Appendix B, "Networks and Routing Basics", to become more familiar with the terminology and procedures used in this manual.

Freecom Technologies • Germany
www.freecom.com

To prevent data loss, make a backup copy of your data each time before reconfiguring the hard drive.

Warning !

 This device was designed for home or office use.

Warning! This device is equipment complying with EN55022 class B.

Freecom Technologies is not liable for any damages that may occur from the use of a Freecom system. We reserve the right to upgrade our products in keeping with technological advances.

GB

User manual

Chapter 1:

Chapter 2:

Chapter 3:

Chapter 4:

Chapter 5:

Apendix:

General Information

Package contents

Please check the contents of the box to ensure it includes following items:

- Freecom FSG drive
- Power pack
- Network cable (UTP)
- Base
- Wall mounting
- CD-ROM with instruction manual and application software
- Quick installation guide
- Safety guide

Technical Support

For any technical questions, please visit our web site at www.freecom.com or at the site created specifically of this product, www.openfsg.com. These websites offer a range of information, answers to frequently asked questions, firmware and product guides (available for download). You can also use our forum to exchange experience with other users or discuss any problems or difficulties you may be having. Or else contact Freecom Support for more in-depth assistance.

Freecom on the net

The FSG and other Freecom products including documentation, drivers, and other information can be found on a World Wide Web home page that you can access at the universal resource locator (URL) http://www.freecom.com. A connection to the Internet and a Web browser such as Internet Explorer or Firefox are required.

Related Publications

There is a lot of information available on the internet that can help you achieve what you want. In this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at www.ietf.org and are mirrored and indexed at many other sites worldwide.

For more information about address assignment, refer to the IETF documents RFC 1597, Address Allocation for Private Internets, and RFC 1466, Guidelines for Management of IP Address Space.

For more information about IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Freecom reserves the right to make changes to the products described in this document without notice. Freecom does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Trademarks

Freecom is a trademark of Freecom Technologies.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

System Requirements

The following hardware and software requirements must be fulfilled to ensure trouble-free operation.

Hardware Requirements

In order to use the Freecom FSG, following components are needed:

- Intel Pentium II 233MHz or higher
- 64MB RAM or higher
- CD-ROM drive for installing drivers and/or software
- LAN
- Internet connection for online warranty registration and driver/software updates and downloads

Software Requirements

- Windows 98 SE
- Windows Me
- Windows 2000
- Windows XP
- Windows NT

- MacOS 8.6 or 9.x
- MacOS X

- Linux Kernel 2.2 or higher

Precautionary measures

To ensure that your Freecom FSG functions properly, please take note of the following precautions. If these are not followed, you may void your warranty and damage the FSG.

- Do not drop the Freecom FSG or expose it to other kinds of sudden mechanical shocks as this may result in data loss and damage to the hard drive.
- Do not use the Freecom FSG when the ambient temperature is below 10°C or above 45°C.
- If the Freecom FSG is moved from a cool environment to a warmer environment, please allow the drive to acclimatize to the ambient temperature before operating the device. Failing to do so may lead to condensation within the drive enclosure, which in turn may cause the drive to malfunction.
- Do not place liquids or drinks on the FSG. When liquids are spilled and get in contact with the electronics within the drive enclosure, it will damage the drive and will cause the drive to malfunction.
- Do not use the FSG in a dusty environment. Dust inside the enclosure may damage the internal electronics and result in drive malfunction.
- Only use the power adapter that was supplied with the FSG.
- Opening the FSG will void the warranty.

Advantages of the Freecom Storage Gateway FSG

The Freecom Storage Gateway is the perfect solution for home and small business use. Thanks to its fast and easy installation, you are up and running the FSG in no time at all.

With its integrated router function, secure Internet access is child's play. Simply plug in a DSL modem on the FSG's WAN port and every computer in the network has access to the Internet immediately. Plus its integrated firewall protects every PC against hackers.

FSG is a combination hard drive, server (3 x LAN, 1 x WLAN) and USB server (4 x USB 2.0 High Speed). This reduces the number of devices you need. Most of the FSG functions can be used with little previous knowledge.

File server

Save your data centrally on FSG and make it accessible to all PCs in the network.

Web server

Save your websites on the FSG and put them directly online.

FTP server

The built-in FTP server allows you to access data from any PC over the Internet.

LAN router

Network several PCs over the three available LAN ports and access the Internet from any computer.

USB server

Increase your storage space by attaching additional devices (e.g., external hard-drives) and let other network devices use this disk space.

USB printer server

Connect a USB printer and use it as your network printer.

Media server

Play multimedia files (films, music, images) on any attached client (for example, the network media player).

Firewall

The integrated firewall protects your data from hackers.

eSATA interface

Connect an external SATA drive such as a hard drive and increase your storage capacity in the process.

Mail server

Use the mail server to set up an individual e-mail account for each user. Users can get their e-mails from an e-mail client through the FSG.

PHP & MySQL

Create forums, guestbooks et al. with PHP and MySQL, and add them to your homepage.

Open Source Firmware

You are familiar with Linux and want to add more features to your FSG? No problem. Firmware is available free of charge and open to modification (The user assumes all risks relating to any modification he/she may perform.).

The Freecom Storage Gateway with 1001 possibilities

The Freecom Storage Gateway replaces many other devices

Software features

Network transport protocols

TCP/IP

Network file protocols

Microsoft Network CIFS

Client support

Microsoft Windows 98/Me/NT 4.0/2000/XP/2003 Server
Apple Macintosh OS 8.x/9.x/10.x

Network settings

DHCP
Manual configuration

System management

Web-based configuration
Configuration wizard

Internet services

HTTP (with PHP)
FTP
SQL
SSH
Mail
UpnP
Dynamic DNS
NTP

Security

Supports user, group and file shares

System configuration

Number of users: unlimited
Number of groups: unlimited

Router

PPPoE
DHCP client
Fixed IP
Firewall
Port forwarding

Hardware features

Processor

Intel XScale IXP422
64 MB RAM
4 MB Flash

Network connection

3x LAN, 1x WAN RJ-45 100 Mbps

USB

4x USB 2.0 480 Mbps for up to four printers or four mass storage devices

S-ATA

1 x eSATA HDD interface

Fan

Temperature-controlled fan

HDD

80/160/250/400/500 GB (depended on model)
HDD sleep mode for lower power consumption and reduced noise

Electrical requirements

Voltage: 100 - 240 V DC
Frequency: 50 - 60 Hz, single-phase

Environmental requirements

Operating temperature: 10 - 45° C (50 - 122° F)
Storage temperature: -10 - 70° C (-40 - 185° F)
Humidity: 20 - 80 % relative humidity, no condensation
Maximum operating altitude (above sea level): 3000 m (9900 ft)

Dimensions and weight

Dimensions: L x W x H: 17.5 x 14 x 4.4 cm / 6.9 x 5.5 x 1.7 inch
Weight: 950 g

Chapter 1: Connecting / Installing FSG

1.1 Hardware Installation

Setup of the FSG is performed using the following steps:

1. Plug the FSG's power cord into a power outlet.

2. Switch on DHCP on the PC, a DHCP server is automatically on on the FSG

3. Connect the included Ethernet Cable into the Ethernet port on the rear of FSG into one of the LAN ports (1,2 or 3). Connect the other end of the cable directly to the PC.

4. Check the LINK/ACT light on the UTP port you have connected on the FSG-3. If it is lit, then your FSG is connected properly.

1.2 Software

The Freecom Storage Gateway wizard quickly detects and performs the basic set-up of your FSG. When you start it, it displays all FSGs available in your network and helps you configure the FSG as a printer server or create network folders.

1. Install the Freecom Storage Gateway Wizard (FSGW) from the enclosed Manual & Application CD.

2. Start the Freecom Storage Gateway Wizard.
3. Check the FSGW whether your FSG was detected. This may take some time. If your FSG is not immediately detected, click "Search again for available Freecom Storage Gateway devices" to repeat the search.

4. For a detailed functional description on the Freecom Storage Gateway Wizard, please refer to chapter 11.

Chapter 2: Get to Know Your FSG

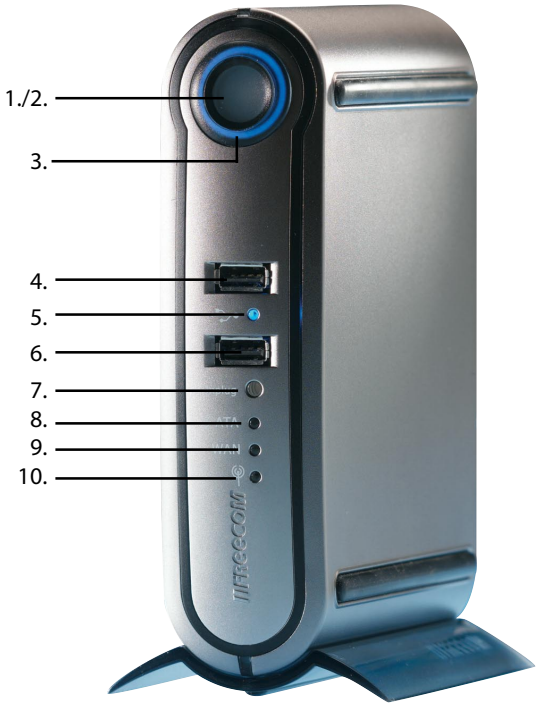
This chapter describes the lights and mechanical layout of the FSG.

2.1 FSG connectors, LEDs and buttons

The FSG Front panel

The front panel consists of:

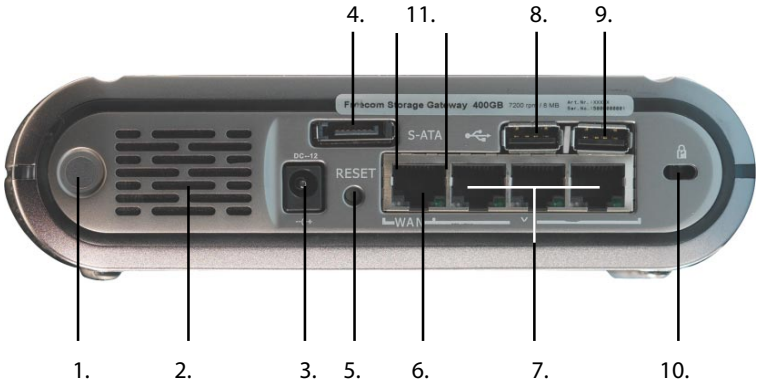
1. Power on
2. Power on LED
3. LED ring
4. USB host port type A (front 1)
5. USB LED
6. USB host port type A (front 2)
7. USB unplug button
8. SATA LED
9. WAN LED
10. WLAN LED



The FSG Back panel

The back panel consists of:

1. WLAN antenna connector
2. Fan inlet
3. 12 V DC power jack
4. eSATA connector
5. Hardware reset button
6. WAN port
7. LAN ports 1, 2 and 3
8. USB host port type A (back 1)
9. USB host port type A (back 2)
10. Kensington lock



Front

Display	POWER (LED SYNC Button)	LED ring	S-ATA LED	WAN LED	WAN LED	USB LED
Solid blue	System boots OK	Normal mode	S-ATA device connected	WAN connected	WLAN is enabled	WLAN is enabled
Flash regularly or intermittently	System boots	HDD activity	-	-	-	-
OFF	System ready or in Standby mode	No power supply	No device connected / Error	No connection / Error	WLAN is disabled	WLAN is disabled

Back

Display	LAN LED		WAN LED	
	Green	Yellow	Green	Yellow
Solid blue	Connection is active	High-speed Ethernet (100 Mbit/s)	Connection is active	High-speed Ethernet (100 Mbit/s)
Flashes intermittently	Possible network collisions	Sending or receiving data	Possible network collisions	Sending or receiving data
OFF	No connection / Error	10 Mbit/s Ethernet	No connection / Error	10 Mbit/s Ethernet

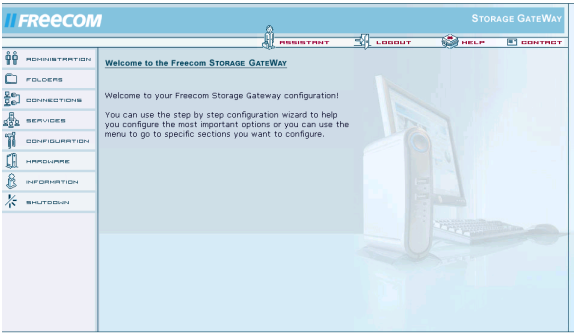
Quick Setup

2.2 FSG configuration wizard

The configuration wizard is integrated into the web interface and helps you to configure the basic settings on your FSG. This in turn ensures you can work with the FSG in the shortest time possible.

2.2.1 Starting the FSG configuration

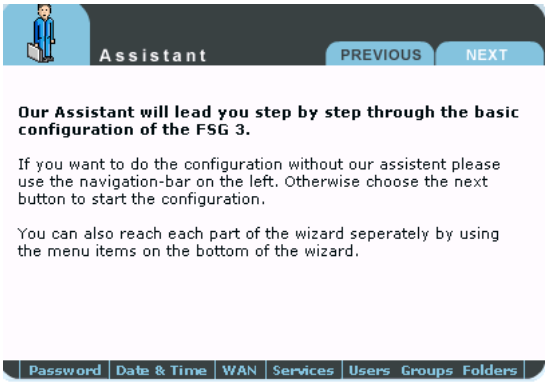
To use the wizard, please go to the configuration page of your FSG by starting any web browser (Internet Explorer, Opera, Firefox etc.) and entering the hostname 'FSG' * or the IP address '192.168.1.1'* in the address bar. Click 'Enter Configuration' and log on under the username 'admin' and the password 'admin'*.



* These are the factory defaults. If you have already changed these settings, enter the new username and password.

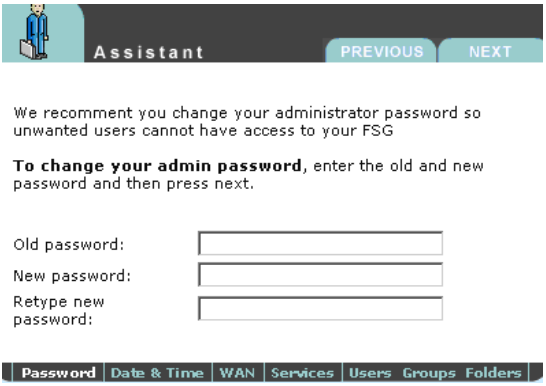
2.2.2 Starting the wizard

Click 'Wizard' in the top menu bar.



2.2.3 Changing the administrator password

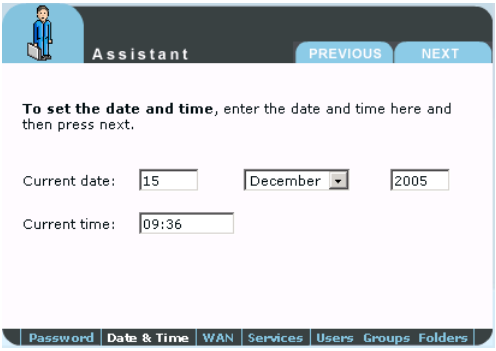
Start the wizard and then click 'Next'. You now have the option of changing the administrator password.



First enter the old password (factory default setting: 'admin') and then type in the new password twice. Now click 'Next'.

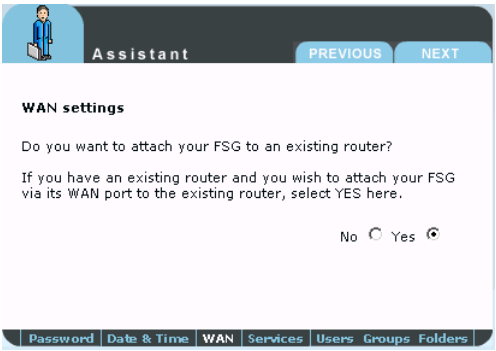
Note: We recommend changing the password because every FSG comes with the administrator password 'admin', in other words any person who knows your IP address could potentially access your FSG.

2.2.4 Changing date and time

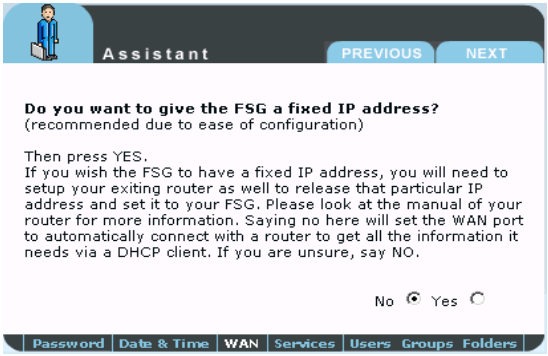


You can change the date and time on the FSG in this window by simply entering the new values and clicking 'Next'.

2.2.5 WAN settings

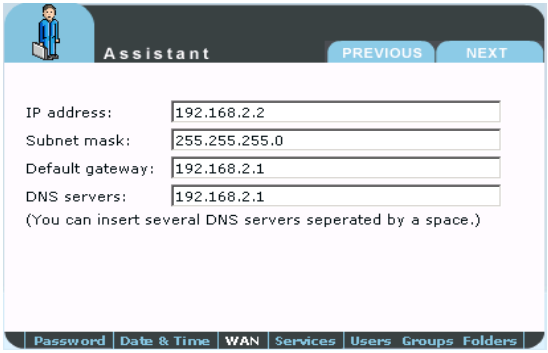


If you are planning to connect the FSG to a router, hit 'Yes' and then 'Next'. If not, press 'No' and then 'Next'.



Do you want your FSG to have a fixed IP address (WAN port)? If yes, select 'Yes' and press 'Next'. If this is not the case, press 'No' and then 'Next'.

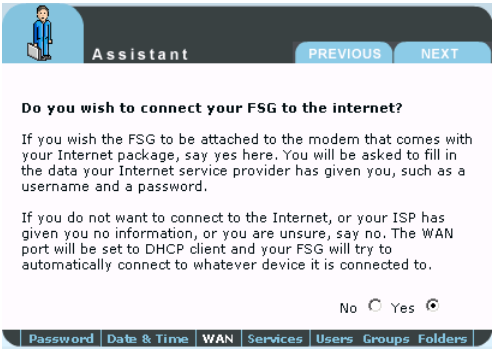
Fixed IP address



You can enter the IP address, subnet mask, Gateway and (multiple) DNS servers to be used by the FSG WAN port in this form.

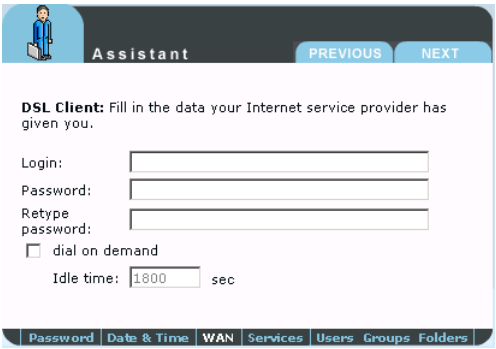
IP address:	Enter an IP address that falls within your router's address range. This IP address provide you with access to the FSG from within your local network.
Subnet mask:	Enter the subnet mask of your router (example: 255.255.255.0).
Standard Gateway:	IP address of your router, e.g., 192.168.2.1.
DNS servers:	Enter the IP address of your router here.

Without router (when selecting 'No')



If you intend to use your FSG as a router and to access the Internet, click 'Yes' and then 'Next'. If not, press 'No' then 'next'.

DSL



You can enter the DSL login data from your provider here and enable 'Dial on demand' if you are using a DSL package with restricted minutes. In this case, the Internet connection is only established when a query is sent to the Internet.

Services

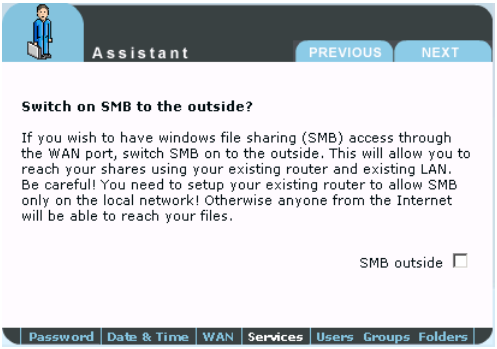
FSG has several useful services which you can configure in the coming sections.

2.2.6 Services

FSG has several useful services which you can configure in the coming sections.

Windows File Sharing (SMB)

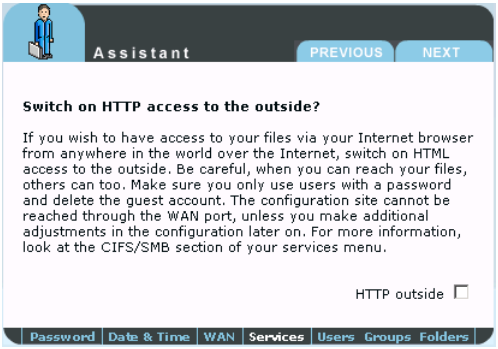
SMB is used by Windows to transfer files and for printing services.



It allows you to enable Windows File Sharing service for the WAN port (for example, to access this via a router).

HTTP server

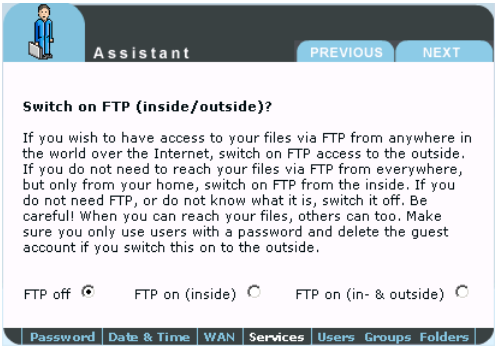
An HTTP server is a server service that provides information in accordance with the HTTP protocol. The data is accessed using HTTP URLs.



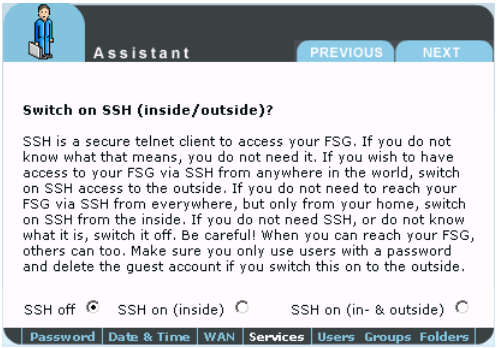
You are given the option here of specifying whether or not the HTTP server can be accessed from outside the network (Internet).

FTP server

You can enable the FTP server and specify whether it can be accessed only internally (within your network) or also from the outside.

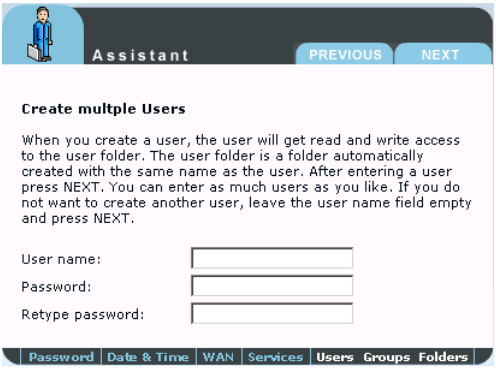


SSH server



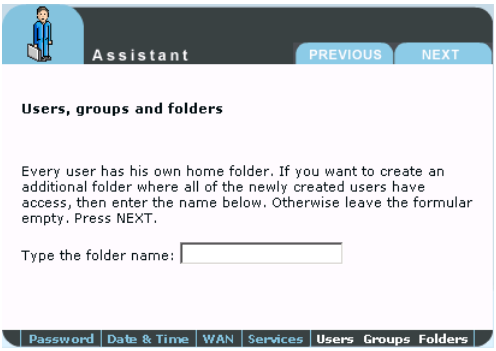
On this screen you can enable the SSH server and specify whether it can be accessed only internally (within your network) or also from outside the network.

2.2.7 Users



You can enter several users with or without a password in this screen. The added users are able to access the FSG via SMB, HTTP or FTP if these services are enabled. If you plan on leaving this area blank, skip to 9.1.9.

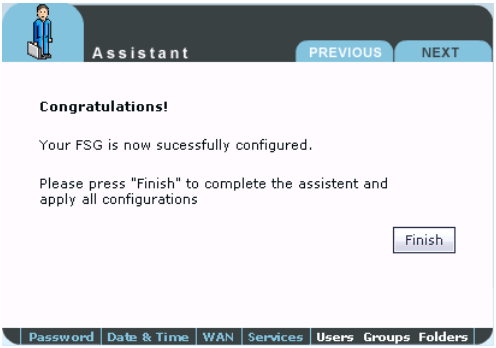
2.2.8 Folders



This screen allows you to create a folder on the FSG. All users added previously have access to this folder.

By creating this folder, you only have to copy files that you want to make available to all users one time to this location. You would otherwise be required to copy these files and paste them in each of individual user folders.

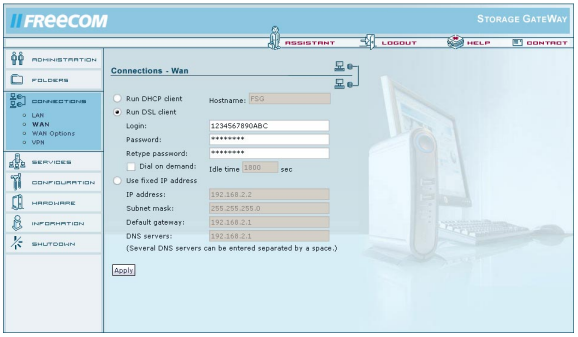
2.2.9 Finish



Click 'Finish' to save your settings.

2.3 Internet access

If you have not already set up your Internet connection in the FSG configuration described above, you may do so at any other time in the future. This is done by clicking 'Connections" – 'WAN' in the FSG menu. Enable 'Run DSL Client' and then enter the login data.



2.4 Accessing data via SMB

Windows

Open Windows Explorer and enter either

\\fsg* or

\\192.168.1.1 in the address bar.

If you have changed the host name or the IP address, please use the new settings.

Enter your username and password for accessing the FSG. If you are logging on as the administrator, you will have access to all folders on the FSG.

Linux

Open the file browser (Konqueror, for instance) and enter

smb://fsg* or

smb://192.168.1.1*

Enter your username and password for accessing the FSG. If you are logging on as the administrator, you will have access to all folders on the FSG.

Mac OS

Mac OS X Vers.10.3 and higher

Select 'Go To' -> 'Connect with Server...'from the menu bar. The FSG address is:

smb://192.168.1.1* or else

smb://FSG_NAME (factory default is smb://FSG).

* Factory defaults. If you have changed the host name or the IP address, please use the new settings.

2.5 Accessing data via SMB

Windows

Open Windows Explorer and enter either

\\fsg* or

\\192.168.1.1

in the address bar.

If you have changed the host name or the IP address, please use the new settings.

Enter your username and password for accessing the FSG. If you are logging on as the administrator, you will have access to all folders on the FSG.

Linux

Open the file browser (Konqueror, for instance) and enter

smb://fsg* or

smb://192.168.1.1*

Enter your username and password for accessing the FSG. If you are logging on as the administrator, you will have access to all folders on the FSG.

Mac OS

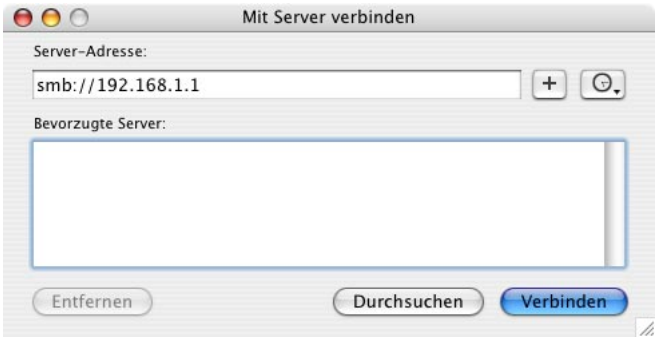
Mac OS X Vers.10.3 and higher

Select 'Go To' -> 'Connect with Server...' from the menu bar. The FSG address is:

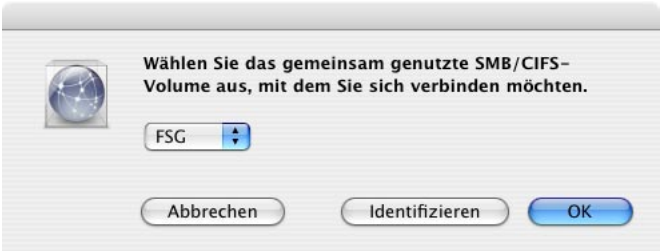
smb://192.168.1.1* or else

smb://FSG_NAME (factory default: smb://FSG).

* Factory defaults. If you have changed the host name or the IP address, please use the new settings.



Click 'Connect'. You now need to select a shared folder on the next screen. Press OK to continue.



Enter the workgroup, your username and password for accessing the FSG. If you are logging on as the administrator, you will have access to all folders on the FSG.

Note: You set the workgroup name of the FSG under 'Connection'-& 'LAN' in FSG Configuration menu.

After pressing OK, the FSG is configured and an icon appears on your computer desktop.

To access all the FSG folders that your username has been assigned user privileges, simply double-click this icon.

2.6 Accessing data via HTTP

Note: You have read but not write access with HTTP.

Local access

Open your browser and enter either "http://fsg"* or "http://192.168.1.1"* in the address bar. Click 'Enter as User' and log on as Admin or as a user. You may now view or download any file in your folder (as a user) or anywhere on the FSG (as the administrator).

Accessing over the Internet

To do so, you need to enable the option 'Open HTTP server to the outside' under 'Services' -> 'HTTP Server' in the FSG configuration menu.

Then open your browser and enter your Internet IP address in the address bar. This can be found in the FSG's configuration menu under 'Information' -> 'Network'-> 'WAN Port' - 'IP Address' if you have connected your FSG directly to a DSL modem. If your FSG is connected to a router, please check in your router's configuration menu.

You may likewise use your DynDNS address (for more information, refer to chapter 10.5.2.

Click 'Enter as User' and log on as Admin or as a user. You may now view and download any file in your folder (as user) or anywhere on the FSG (as administrator).

* If you have changed the hostname or the IP address of the FSG, please use the new settings here.

2.7 Accessing data via FTP

Note: Not all browsers can upload data via FTP. Those that can include Internet Explorer and Konqueror. We recommend using FTP client software such as WS_FTP, SmartFTP or CuteFTP.

Local access

Enable the FTP Server option (Service -> FTP Server - Run FTP server). Use any FTP client software or open your browser and enter

ftp://USERNAME:USERPASSWORD@192.168.1.1

or

ftp://USERNAME:USERPASSWORD@fsg.

Accessing via the Internet

Enable FTP for the Internet (Service -> FTP Server -> Open FTP server for the outside). Use any FTP client software or open your browser and enter

ftp://USERNAME:USERPASSWORD@YOUR_INTERNET_IP

or

ftp://USERNAME:USERPASSWORD@YOUR_DYNDNS_HOST.

USERNAME = your username

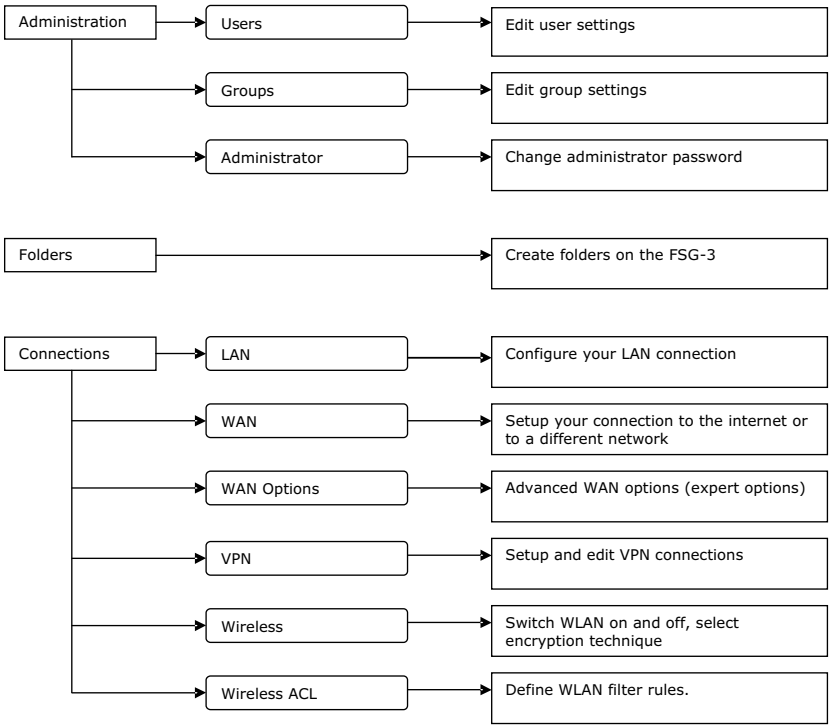
USERPASSWORD = your user password

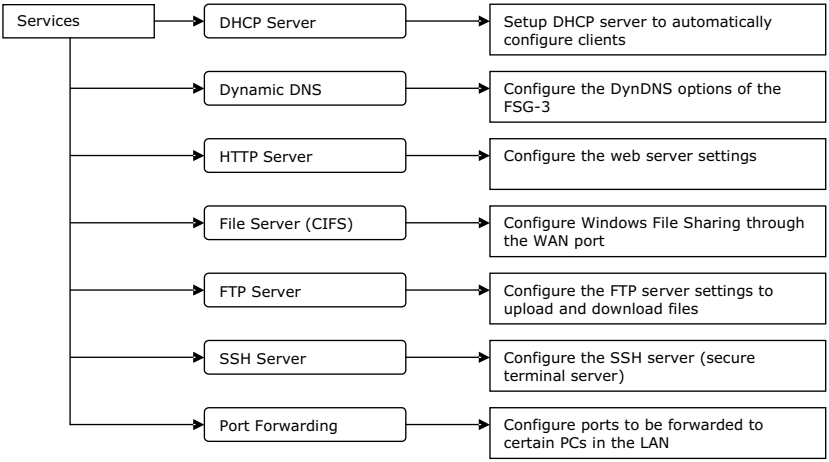
YOUR_INTERNET_IP = your WAN IP address

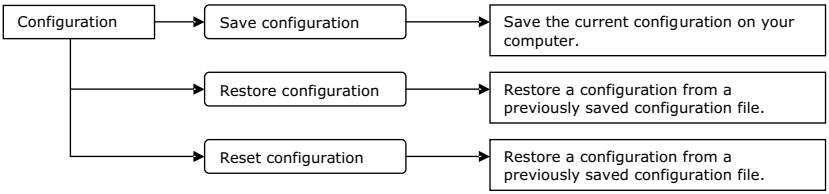
YOUR_DYNDNS_HOST = your Dynamic DNS address

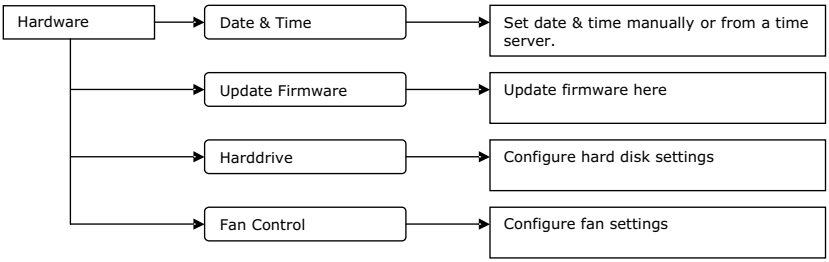
Chapter 3: FSG Functions

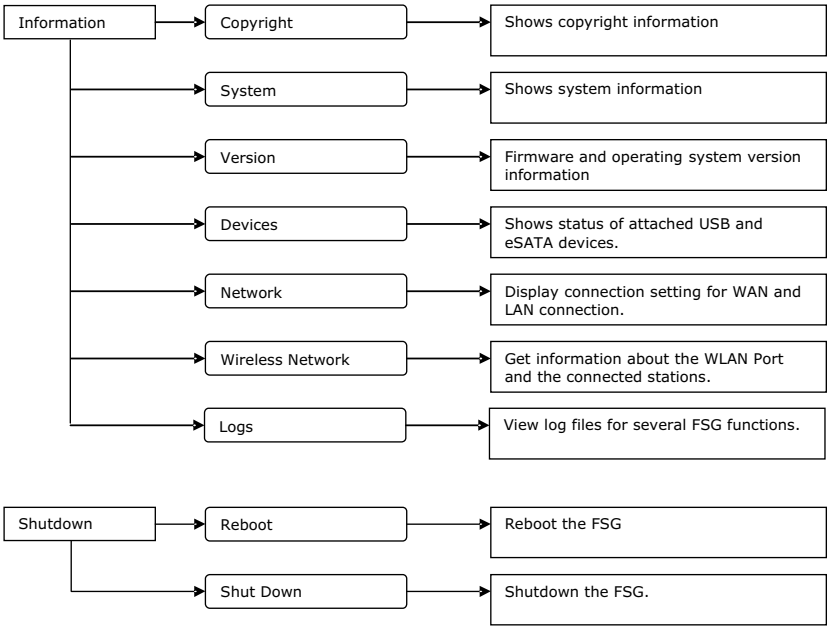
3.1 Overview




Services
DHCP Server
Setup DHCP server to automatically configure clients
Dynamic DNS
Configure the DynDNS options of the FSG-3
HTTP Server
Configure the web server settings
File Server (CIFS)
Configure Windows File Sharing through the WAN port
FTP Server
Configure the FTP server settings to upload and download files
SSH Server
Configure the SSH server (secure terminal server)
Port Forwarding
Configure ports to be forwarded to certain PCs in the LAN


Configuration
Save configuration
Save the current configuration on your computer.
Restore configuration
Restore a configuration from a previously saved configuration file.
Reset configuration
Restore a configuration from a previously saved configuration file.


Hardware
Date & Time
Set date & time manually or from a time server.
Update Firmware
Update firmware here
Harddrive
Configure hard disk settings
Fan Control
Configure fan settings


Information
Copyright
Shows copyright information
System
Shows system information
Version
Firmware and operating system version information
Devices
Shows status of attached USB and eSATA devices.
Network
Display connection setting for WAN and LAN connection.
Wireless Network
Get information about the WLAN Port and the connected stations.
Logs
View log files for several FSG functions.
Shutdown
Reboot
Reboot the FSG
Shut Down
Shutdown the FSG.

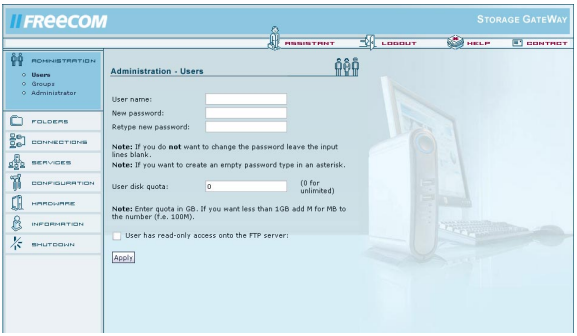
3.2 Administration

3.2.1 Users

Go to Administration -> Users.

You can manage access privileges to the FSG by creating new users.

- When you click 'New', a dialog box appears on the screen where you can add new users.
  - Enter a username and password.
  - Confirm the password.
  - In the 'User disk quota' field, you can limit the storage space for each user. For instance, enter '50' (50 GB) or 50m (50 MB) as the limit. If you enter '0', the user is given unlimited space on the FSG.



Note: The allocated space only includes files personally added by the user and not those entered by others. If, for instance, the administrator writes data to the user's folder, this does not count towards the user's total allotment.

- To grant the user read-only access, click 'User has read-only access onto the FTP server'. If this field is not enabled, the user has read and write access.

- To edit the user settings at a later time, click the user followed by the 'Properties' button.
- To remove this user, click this entry followed by the 'Delete' button.

Please confirm that you really want to perform this operation by pressing 'Yes, I want to delete the user and all its data'.

3.2.2 Groups

Go to Administration -> Groups.

Access control for all file access systems (FTP, HTTP and SMB) is structured around either group or user access rights (privileges). You can add or remove access rights in this window. If a group is assigned privileges or has them revoked, these are assigned / revoked for all users in this group.

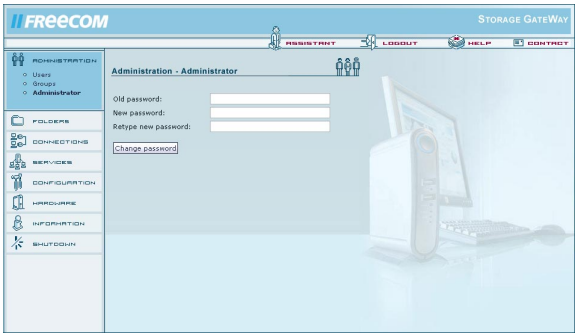
- When you click 'New', a dialog box appears on the screen where you can add new groups.
- You can add new users or edit the group settings by selecting a group and clicking the 'Properties' button.
- If you select a group and hit the 'Delete' button, the group, but not the users in the group, is deleted.

3.2.3 Administrator

Go to Administration -> Administrator.

Here you can alter the administrator password. Please enter the old password, the new password and a retype of the new password.

If you have completely lost your administrator password, please do a reset to default values as described in Reset.

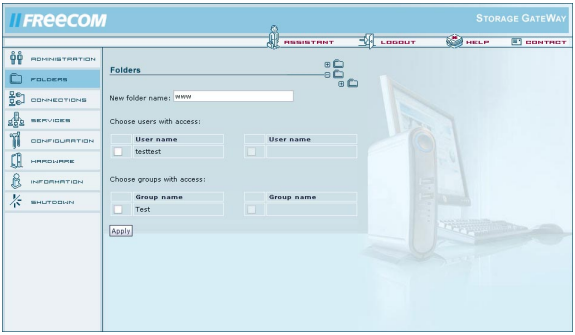


3.3 Folders

Go to 'Folders'.

The access control for all file retrieval systems (FTP, HTTP and SMB) is based on either group or user access rights. Access permissions can be set or removed using these menus. Folder permissions can be given either to a group or a user or both.

- Pressing the Add button gives you a dialog to add new folders. These folders will be created.
- Selecting a folder and pressing the properties button will allow you to edit the folder settings and add groups or users.
- Selecting a folder and pressing the delete button will delete the folder.



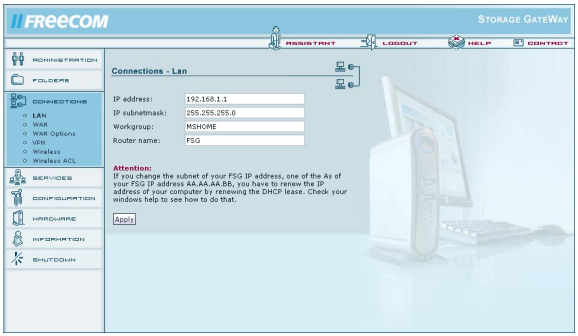
3.4 Connections

3.4.1 LAN

Go to Connections –> LAN.

Here you can set up your connection to the local area network (LAN).

Options	Description
IP address	This is the IP address your FSG uses in your LAN
IP subnet mask	This is your subnet mask
Workgroup	This is the name of the workgroup where your FSG is located.
Router name	Name of the FSG in the LAN. This name can be used to access the web configuration (e.g. http://FSG) instead of using the IP address. This makes it easier for the user to access the web interface.

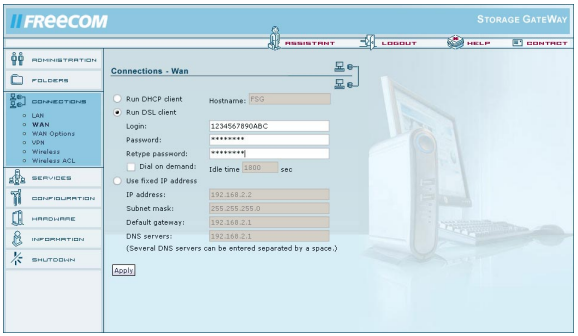


3.4.2 WAN

Go to Connections –> WAN.

You can configure your connection to the Internet or any other network on this screen.

Options	Description
Run DHCP Client	Enables the DHCP Client option. If the WAN port is connected to a DHCP server (e.g., another router), you will need to set up the WAN connection using this option.
Run DSL Client	If the WAN port is connected directly to a DSL or cable modem, you will need to enter information provided by your provider in several fields. This option allows you to set up PPPoE or other types of DSL or cable connections.
Login	Username that you received from your ISP.
Password	Password that you received from your ISP.
Retype Password	Re-enter your password that you received from your ISP.
Dial on Demand	A DSL connection is established only when a PC in the network requests one.
Idle time (in seconds)	Use this option if you are only given a limited contingent of online hours each month. The DSL connection is disconnected if the user does not send or receive data within a set period of time (in seconds).
Use fixed IP	This allows you to manually enter the IP address for thenetwork connection. This is your fixed IP address; please ask your ISP or network manager for this information.
Subnet mask	Subnet mask; please ask your ISP or network manager for this information.
Default gateway	Your ISP's gateway address; please ask your ISP or network manager for this information. If your FSG is connected to a router, please enter the router's IP address in this field.
DNS servers	Your ISP's DNS server address; please ask your ISP or network manager for this information. If your FSG is connected behind a router, please enter the router's IP address in this field.

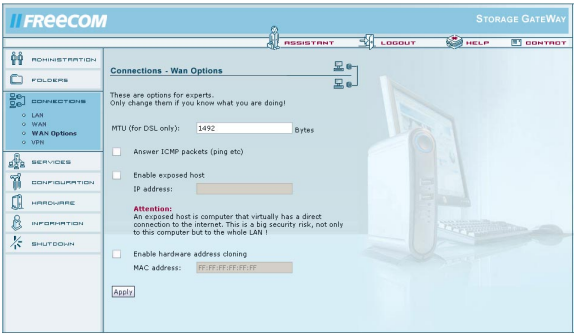


3.4.3 WAN options

Go to Connections –> WAN Options.

ATTENTION: These options are intended for expert users only. Only change these settings if you know what you are doing!

Options	Description
MTU (for DSL only) (In Bytes)	MTU settings (MTU = Maximum Transfer Unit)
Answer ICMP packets (ping etc)	This will allow others to ping the host. It is good for debugging but it can be asecurity hazard!
Enable exposed host	Enabling this will allow one PC on the LAN to act as if it bypasses the firewall completely and has a direct connection to the internet (Attention: An exposed host is computer that virtually has a direct connection to the internet. This is a big security risk, not only to this computer but to the whole LAN!).
IP address	Exposed host IP address.
Enable hardware address cloning	This will enable you to set the MAC address of the WAN connection so it matches the address your ISP authenti-cates by.
MAC address	This is the MAC address your WAN port will be cloned to.
Open SBM/CIFS on WAN port	This will open SMB/CIFS for the WAN port. Only needs to be enabled when the FSG is used behind a router.



3.4.4 VPN

Go to Connections –> VPN.

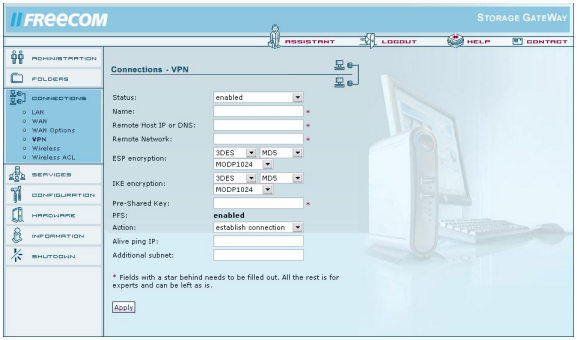
The VPN connections listed here are shown with name, status, operation, Remote Host and Remote Net.

- If you are adding a new dedicated connection, click 'Add connection'.
- To view and edit the properties of the existing connection, select the connection and click 'Properties'.
- To remove a connection, click 'Delete connection'.
- To view the status of your connections, click 'Show status'.

Adding a new connection

To add a new VPN connection, click the 'Add connection' button.

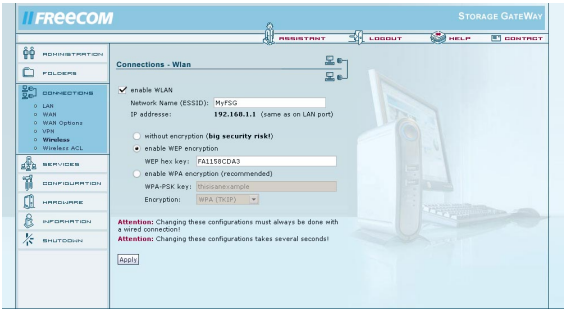
Options	Description
Status	You can choose to enable or disable the connection.
Name*	This is the name which will refer to the VPN connection. It is used for internal use only.
Remote Host IP*	This is the IP address of the remote host you wish to reach. If you which to allow any IP (Road Warrior) type enter: 0.0.0.0.
Remote Network*	This is the remote network you wish to reach. Example: 192.168.20.0/24
ESP encryption	ESP encryption options
IKE encryption	IKE encryption options
Pre-Shared Key	Fill in your pre-shared key here. Please ask your network administrator for more info
Action	You can specify if you want a listening only connection or a full connection.
Alive ping IP	Here you can enter an IP address where a ping is sent every 15 minutes. This maintains a connection whenever the server times out due to lack of activity on the other side.
Additional subnet	If you want to route another subnet via the VPN tunnel, enter its IP address here (e.g., 192.168.50.0/24).



* Fields with an asterisk (*) need to be filled out. All the rest is for experts and can be left as is.

3.4.5 WLAN

Wireless LAN (WLAN) is a network structure that does not utilize any cables. WLAN allows you to connect your FSG to other WLAN-capable mobile devices.



enable WLAN	Enable and disable WLAN.
Network Name (ESSID)	The name of the network identified by the FSG (any name can be entered here).
IP address	Shows the LAN IP of your FSG.
without encryption	Sets the FSG connection type to no encryption. Using this type of connection may present a serious security risk because all WLAN-capable devices in your network are able to access your shared **directories, files, and Internet connection!** Only use this connection type for test purposes and do not use it under any circumstances if your FSG contains confidential information.

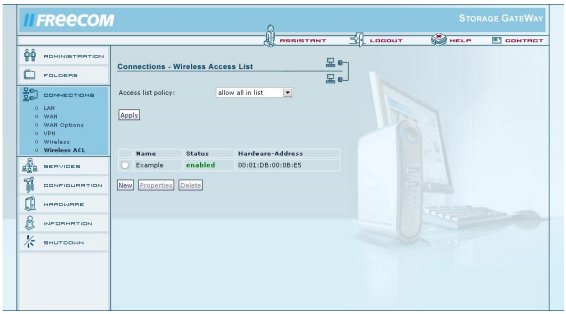
enable WEP encryption	The Wired Equivalent Privacy, or WEP encryption for short, enables you to protect your FSG connection against unintended access. The WEP key has to be either 10 or 26 characters in length and use the hexadecimal format. Characters permitted: 0123456789ABCDEF. Please write down the code you have entered. This needs to be entered on all of the devices that access your FSG. An example of a 10-character code: FF37AC99B1 **Do not use the code provided above.** You should only use WEP if your terminal device does not support WPA encryption as the WEP standard is out-of-date and not secure.
enable WPA encryption	Wi-Fi Protected Access (WPA) is an encrypted connection type that protects your network against unintended access. If you intend to use WAP, you will need to create an authorization key used by the devices to log on to your FSG. Please make a note of the key. We highly recommend using WAP encryption.
WPA-PSK key	You need to enter an authorization key in this window if the 'WAP encryption' option is enabled. This is used by the devices to log on to your FSG via WLAN. PSF, short for PreShared Key, is a WEP protocol extension. The key should contain no less than 8 and no more than 63 characters.

encryption	You can choose the type of encryption for the selected key type from this drop down menu.
	The following options are available:
WPA (TKIP)	TKIP is the most basic method of encryption in WPA. All devices that support WPA can use this method.
WPA2 CCMP	WPA2 is an upgraded version of WPA. The method of encryption is an enhanced version of WPA. WPA2 is however not supported by all devices.
WPA and WPA2	When this option is selected, your FSG determines which method to use to connect a device to your FSG.

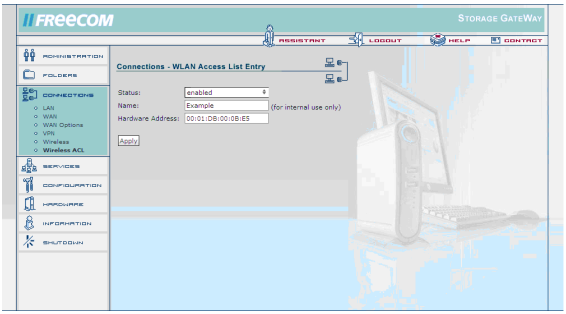
3.4.6 Wireless ACL

Wireless ALC enables you to filter devices attempting to access your WLANs based on their MAC address. This method of access filtering is not secure and should only be used in combination with WPA as many devices allow the user to manually change the MAC address.

Access list policy	This option allows you to set the connection filter for WLAN access. This option filters the devices according to their MAC address and is therefore not secure!



Open to every client	When this option is selected, no type of filtering takes place. All devices can connect to your FSG.
allow all in list	All devices in the filter list are granted access.
deny all in list	All devices contained in the filter list are denied access.
New	Press the 'New' button to add devices to the filter list.
Properties	This properties window allows you to edit the settings for your filter entries.
Delete	Press 'Delete' to remove the selected filter entry from the list.



Status:	enabled: activates the filter; disabled: deactivates the filter
Name:	You enter a name for the filter here in this field.
Hardware address	The user needs to enter the MAC address for these filter rules (MAC address) (see example).

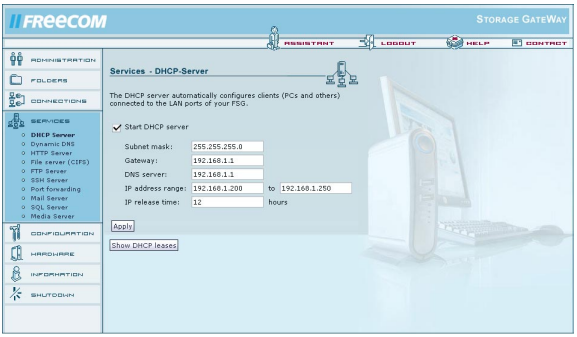
3.5 Services

3.5.1 DHCP server

Go to Services –> DHCP Server.

The DHCP server is responsible for giving dynamic IP addresses to the computers on the LAN. For more information, please read Networks and Router Basics.

Options	Description
Start DHCP server	Check this if you want to run the DHCP server. Do not run the DHCP server if you use fixed IP addresses.
Subnet mask	The subnet mask in use for the DHCP server.
Gateway	The IP address of the gateway the DHCP clients should be automatically forwarded to if they want to reach external sites. This address should usually be the FSG itself, unless a different gateway is running.
Domain name server	The IP address of the DNS server the clients should query. This should be the FSG IP address or an other DNS system.
IP address range	The range of IP addresses the DHCP server can use.
IP release time	The time between refreshing IP addresses given to DHCP clients.



3.5.2 Dynamic DNS

Go to Services -> Dynamic DNS.

Dynamic Domain Name System gives the ability to provide an official DNS name such as www.yourname.com to the dynamic IP address you have gotten from your ISP. You will need to register at one of the listed providers. Please see their websites for further details.

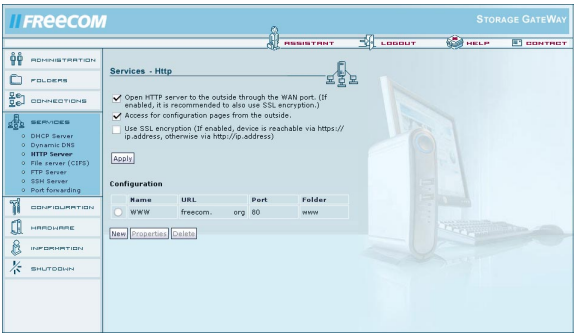
Options	Description
Run dynamic DNS client	Check this if you want to enable the Dynamic DNS client
Service	Several different Service providers are supported. These are dyndns.org, dtdns.com, no-ip.com. Register at the website of one of the service providers and fill in the required information
Host	This is the domain name you registered at the DDNS service provider
Username	This is the username you registered at the DDNS service provider
Password	This is the password you registered at the DDNS service provider
Retype password	This is the password you registered at the DDNS service provider again

3.5.3 HTTP Server

Go to Services -> HTTP Server.

Use these settings to configure the web server. The web server in use is a version of Apache.

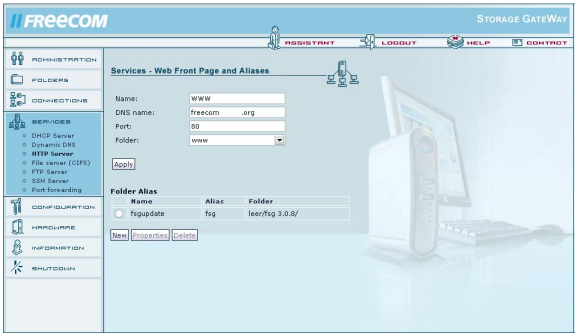
Options	Description
Open HTTP server to the outside	This allows the http server to be reached from IP addresses whose source address is located somewhere on the internet (if enabled, it is recommended to use SSL encryption as well).
Use SSL encryption	This will allow SSL encrypted pages (https) This is a security feature (If enabled, device is reachable via https://ip.address, otherwise via http://ip.address).
Access for configuration pages from the outside	Provides access to the FSG web interface from the outside. (e.g., Internet)
Configuration	You open and configure the existing Web Front Pages here.



Web Front Pages and Aliases

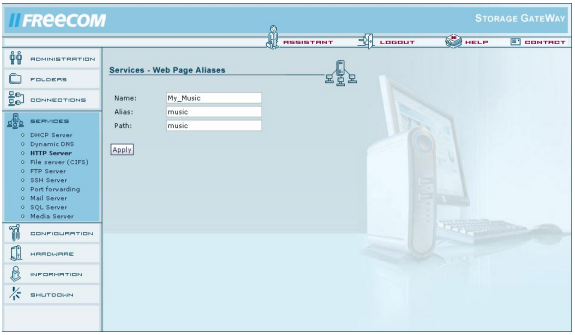
Go to Services -> HTTP Server -> Configuration -> New.

Options	Explanation
Name	Enter a name for your homepage here.
DNS Name	Enter the DNS name for the homepage that you registered with a Dynamic DNS provider.
Port	Enter the port that you want to use to access your homepage. (We recommend using port 80. If another port is selected, you will need to enter the port each time you access the page. Example: hhtp:ip-address:81 for port 81.)
Folder	Select the folder where your homepage is stored.
Enable PHP 4	Enables PHP-4 support for this DNS name.



Web Page Aliases

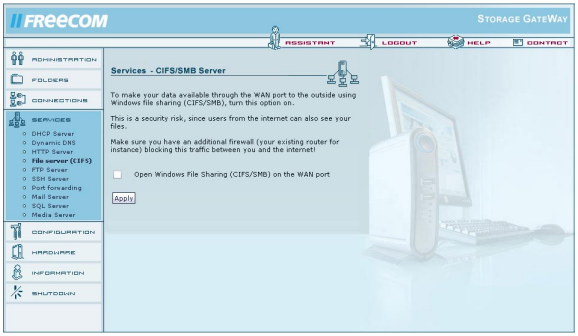
Options	Explanation
Name	Enter a name for your alias.
Alias	Enter a name used to access your alias (e.g., music) if you want your alias to be reached at www.yourname.com/music.
Path	Enter the folder path on the FSG used to access the alias.



3.5.4 File Server (CIFS)

Go to Services -> File Server (CIFS).

You can enable Windows File Sharing for the outside via the WAN port on this screen. This enables you to access your FSG over the Internet using Windows Explorer by entering your Dynamic DNS hostname. This is done by typing in \\www.yourname.com in the address bar (type in your Dynamic DNS hostname instead of www.yourname.com).

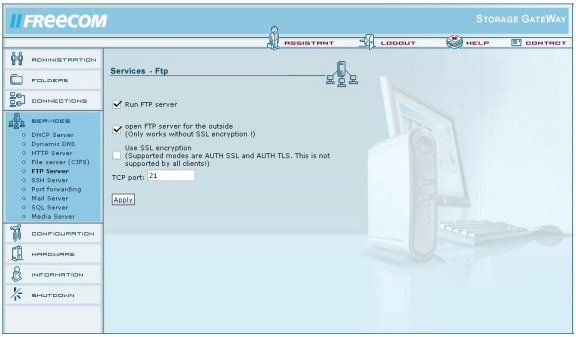


3.5.5 FTP Server

Go to Services -> FTP Server.

This is a File Transfer Protocol (FTP) based server.

Options	Explanation
run FTP server	Turn on the FTP server.
open FTP server for the outside	The FTP server may now be accessed by Internet users from the outside (only functions internally, not in the Internet).
Use SSL encryption	Activates SSL encryption for FTP. Is not supported by all browsers.
TCP port	Enter a port here if you do not want to use the default port for FTP (port 21).



3.5.6 SSH Server

Go to Services -> SSH Server.

The SSH server is a secure terminal client that can be used to perform advanced configuration settings. Please only use this where required because it may present a security risk. All users with a user account on the FSG can access the FSG.

Options	Explanation
Run SSH server	Start/stop server
Open SSH server to the outside	The SSH may now be accessed by outside Internet users through the WAN port.

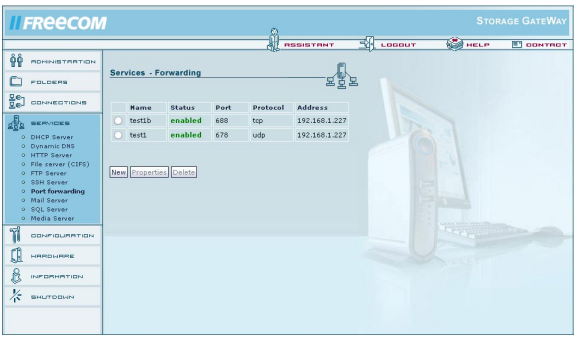
Attention: Starting the SSH server represents a security risk. Only do this if you trust the users!

3.5.7 Port forwarding

Go to Services -> Port forwarding.

Port forwarding is a type of NAT (Network Address Translation). It permits certain ports to access select PCs within the local area network from the Internet. This is a method used to circumvent the firewall. The list indicates which ports are forwarded to which IP addresses in the LAN. Click 'New' to create a new port forwarding.

Options	**Explanation**
Name	Can be any random name.
Status	Shows the status of port forwarding for the requested port (enabled or disabled).
Port	You can enter the port(s) that you want to forward to the PC with the IP address as indicated below. You can enter several ports separated by commas (e.g., 21, 23, 80). If you enter a colon, a range of ports is selected (e.g., 2600:2700).
Protocol	Shows the protocol selected for the forwarding port (TCP or UDP).
IP address	Shows the internal IP address of the PC the port is forwarded to.



3.5.8 Mail server

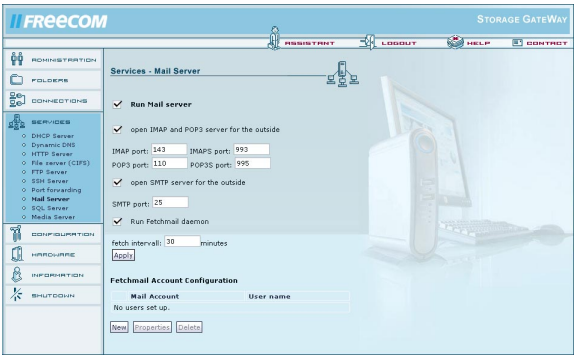
Select Services -> Mail Server.

The mail server allows you to set up provider independent e-mail addresses for use by individuals using your FSG. If you do not have your own domain name, you may also use a Dynamic DNS address here. Example: Your DynDNS address is test.yourdyndns.org. The admin e-mail address in the case would be admin@testyourdyndns.org.

Fetchmail allows you to retrieve e-mails from other accounts and manage them centrally on your FSG.

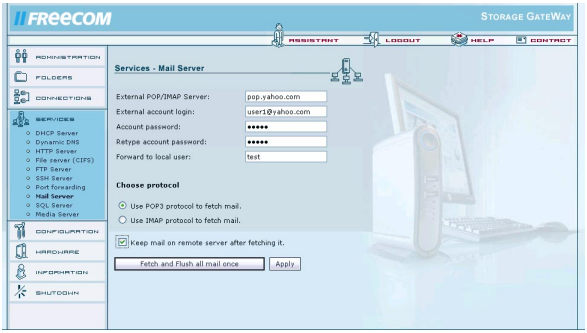
For more details on using the mail server, please refer to the chapter 'Setting up the FSG Mail Server'.

Options	Explanation
Run Mail Server	Enables the mail server.
Open IMAP and POP3 server for the outside	Permits the use of IMAP and POP3 via the WAN port.
Open SMTP server for the outside	Permits the use of SMTP via the WAN port.
Run Fetchmail daemon	Starts Fetchmail. Fetchmail allows you to get e-mails from other e-mail accounts and allocate them to specific FSG users. Fetchmail checks all accounts at preset intervals for new e-mails.



To set up Fetchmail, click 'New' in the 'Fetchmail Account Configuration' section. You need to enter the details required to retrieve e-mails here.

Options	**Explanation**
External / Account Login	Enter an e-mail account from which the e-mails are retrieved.
External POP/IMAP Server	Enter the POP/IMAP server for the e-mail account.
Account password	Set the password for the e-mail account.
Retype account password	Re-enter the password for the e-mail account.
Forward to local user	Enter the name of the user's mail folder where the mail is forwarded (local FSG user).
Choose protocol	Select whether to use POP3 or IMAP for fetching e-mails. Note: Many freemail providers only support POP3.
Keep mail on remote server after fetching it	Enable this option if you do not want the e-mails to be deleted from the server after retrieval.



3.5.9 SQL server

Go to Services -> SQL Server.

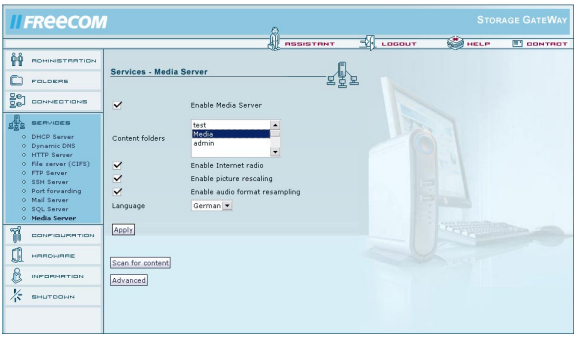
The SQL server allows you to create and manage databases via SQL. In this case, use a MySQL client or a PHP script.

Options	Explanation
Run SQL server	Activates the SQL server.
Open SQL server for the outside	Allows you to use the SQL server via the WAN port.
TCP Port	The TCP port used for SQL queries.
Administration page	Opens the Configuration window where databases and users are configured.
SQL Administrator	If you are no longer able to access SQL when for instance the user has been deleted, you can set up a new administrator account.
Password	Set the password for the SQL administrator in this field.
Re-type password	Re-enter the password for the SQL administrator.
Set Account	Click here to set up the SQL administrator account.

3.5.10 Media server

Open Services -> Media Server.

Options	Explanation
Enable Media Server	Activate the media server.
Content Folders	Display a list of folders on the FSG.
Enable Internet Radio	Enables the use of Internet radio through the FSG.
Enable Picture Rescaling	Enables you to automatically resize images.
Enable audio format resampling	Enables you to resample various audio formats.
Language	Menu language for 'Advanced Options'.



3.6 Configuration

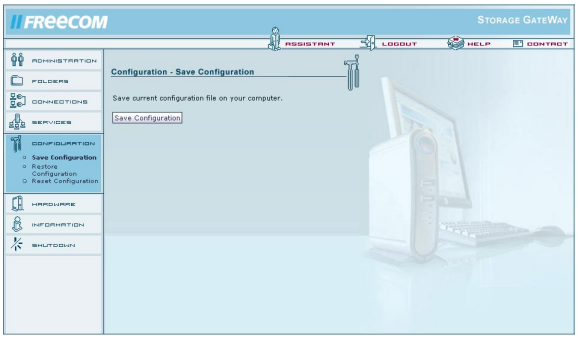
It is possible to save and restore all FSG user settings.

Note: Please do not save your user settings directly on the FSG.

3.6.1 Save configuration

Open Configuration -> Save Configuration.

In this window, you can save the current configuration file on your computer.

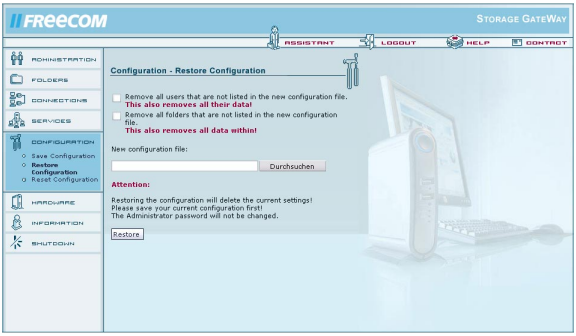


After pressing the button, you are asked where you want to save the back-up copy of the configuration file. Select a location and click 'Save Configuration'.

3.6.2 Restore Configuration

Open Configuration -> Restore Configuration.

This window offers you the option of restoring a previously saved configuration file.



Press 'Browse' to select an existing backup copy of your configuration file. Then click the 'Restore' button to start the process.

Do not turn the FSG off while the configuration is being restored. This will corrupt and destroy the configuration of your FSG.

A button is provided that allows you to delete all users not found in the restored configuration. All data in these directories is then deleted! If you do not press this button, the user data and logins are not deleted.

You may also select whether to delete the folders of your FSG that do not exist in the restored configuration. All data in these folders is then deleted!

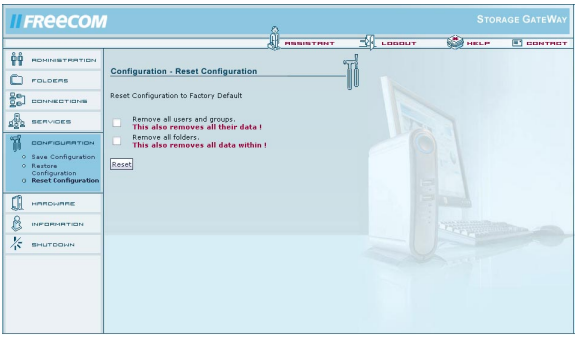
Attention: Please keep in mind that any changes you may have made to the configuration after backing up the restored configuration will be deleted.

Attention: If the Restore Configuration option is enabled, all existing settings will be lost! Please save the current configuration beforehand! The administrator password remains unchanged.

3.6.3 Reset configuration

Open Configuration -> Reset Configuration.

Please click the reset button to reset the factory default configuration. This does not affect or change the version of firmware. You can delete all users.



You can delete all users and groups with one button. All data is then deleted! If this option is not selected, the user data and logins are not deleted. You may also choose to delete all folders on your FSG. All data in these folders is then erased!

Attention: Removing all users and folders also means that this data is lost.

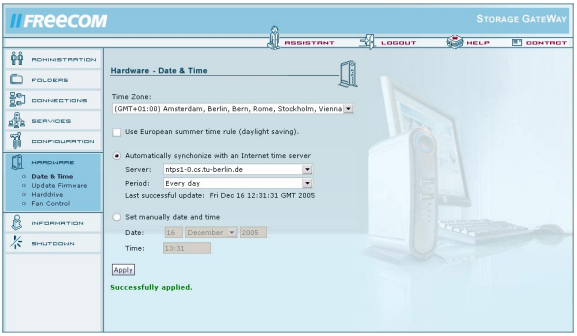
To reset the hardware, press the Reset button located on the back of the FSG. Do this for instance when you are no longer able to access the web interface. When you press the Reset button, the administrator password is also reset to 'admin'.

3.7 Hardware

3.7.1 Date & Time

Open Hardware -> Date & Time.

You may change the date and time on the FSG here. You may change the settings manually or use the Internet time server.



Options	Explanation
Time Zone	Select your local time zone.
Use European summer rule	Enable this option if you live in a country that uses time summer time.
Automatically synchronize with an Internet time server	When using this option, select a time server and update interval.
Set manually date and time	If you enable this option, please set the date and time manually.

3.7.2 Update firmware

Open Hardware -> Update Firmware.

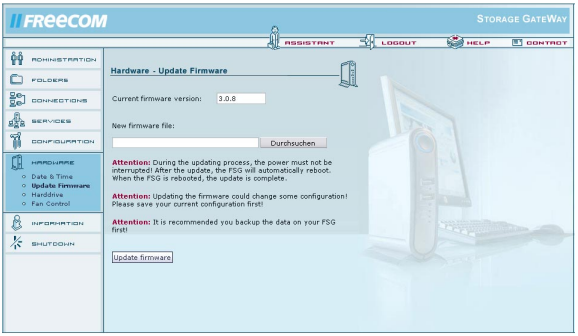
Here you can update the firmware. New firmware usually fixes bugs and adds additional features to your FSG. Check on www.freecom.com if new firmware updates are available for the Freecom Storage Gateway.

Freecom will release new and updated firmware on a regular basis. It is also possible to obtain the source code and create your own firmware.

Attention: Changing the source code of the firmware is at your own risk!

Download the firmware file and click on "Browse" to select the file. Click on "Update firmware" to start the update.

Attention: Updating the firmware is at your own risk! Make sure to make a backup of your current configuration before updating the firmware.



3.7.3 Hard drive

Open Hardware -> Harddrive.

You can configure any hard drive setting in this window.

Spin-down time

Hard drives are devices with moving part that create noise and heat, and consume power. If the FSG is not used for an extended period of time, your best option may be to shut down the hard drive. This reduces power consumption and the amount of noise and heat generated. It also increases the operational life of the hard drive. When the hard drive is shutdown, it will take longer to access it initially because the hard drive has to first start spinning.

You can set the time after which the hard disk shuts down following the last access. If you do not want to use this option, please enter 0.

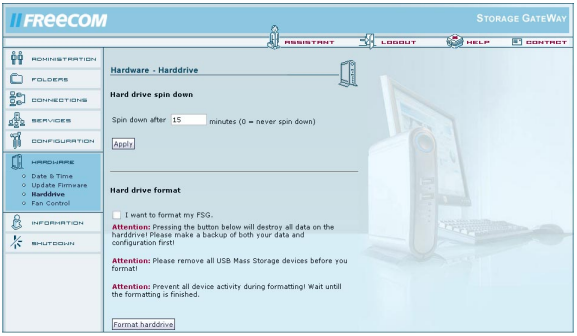
Once you have set the time, click 'Apply'.

Formatting the hard drive

Before formatting the internal HD on the FSG, please read the warning notices. All data is lost during formatting! After reading the warning notices, please press the button to confirm you want to format the hard drive. Then click the 'Format drive' button.

Attention: When you click the 'Format drive' button, all data on the drive is lost! Please make a backup copy before formatting the drive.

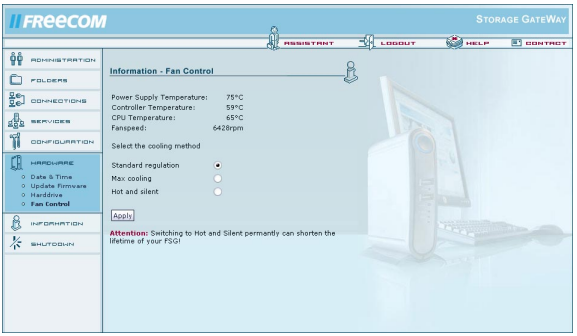
Attention: Stop all operations on the device while the drive is being formatted!



3.7.4 Fan control

Open Hardware -> Fan Control.

This option allows you to adjust the fan speed. Reducing the fan speed means less noise, but higher temperatures in the device. When operating the device in extremely warm conditions or whenever the device is in constant use, we recommend that you increase the fan speed to deliver more cooling capacity.

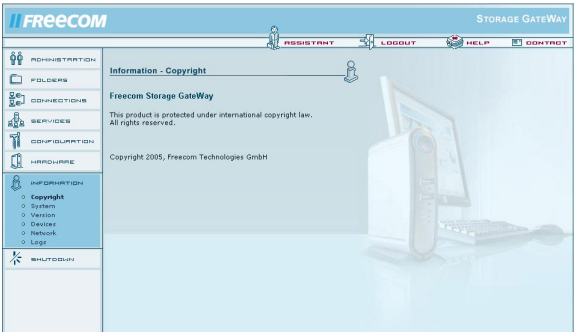


3.8 Information

This is the information menu. It contains diagnostics data and general information.

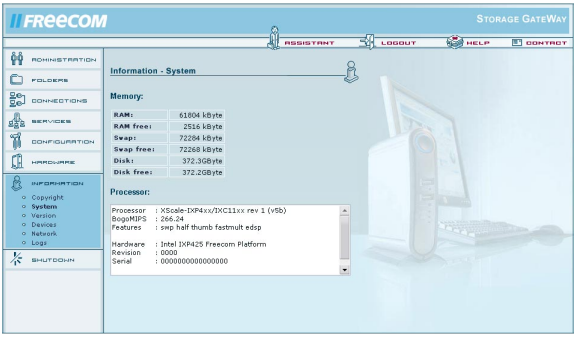
3.8.1 Copyright

Open Information -> Copyright.
This section contains information on copyrights for your FSG.



3.8.2 System

Open Information -> System.
You will find general system information on available disk space and your processor.



3.8.3 Version

Open Information -> Version.

This window displays information on the operating system and firmware contained on FSG.

3.8.4 Devices

Open Information -> Devices.

This dialog box displays a list of attached devices. Click 'Refresh' in your browser if one of the connected devices is not displayed on the screen.

Note: eSATA are only detected by the FSG once it has been restarted after the device is attached. After restarted the FSG, the eSATA device is detected and is then ready for use.

3.8.5 Network

Open Information -> Network.

Both LAN and WAN (internet) Network information is found here for the FSG. If you need the IP address of the FSG, please look for it here.

WAN Port:

Status	Shows the active status
Hardware Address	Shows the MAC address or physical address of the port
IP Address	Your outside FSG (WAN) internet IP address assigned by your ISP
Broadcast Address	This address is used to ask all computers on a subnet at once
Subnet Mask	This is the subnet mask gotten from your ISP
Cable Attached	This shows if the cable is attached or not

LAN Port:

Hardware Address	Shows the MAC address or physical address of the port
IP Address	Your FSG (LAN) internet IP address
Broadcast Address	This address is used to ask all computers on a subnet at once
Subnet Mask	This is the subnet mask you setup for your network

DNS servers:

Displays a list of DNS servers assigned to you by your provider.

3.8.6 Logs

Open Information -> Logs.

If you encounter problems with you FSG, you can use the log file recording option to locate the issue.

The FSG offers several log files for different software components:

- Kernel
- DSL connection
- DHCP server
- Hotplug
- VPN connections
- Dynamic DNS
- FTP server
- E-mail server

To enable the log function, simply hit the 'Start log file recording' and then press 'Apply'. Select a function (e.g., DSL connection) from the list and click 'Refresh' to update the screen display.

3.9 Shutdown

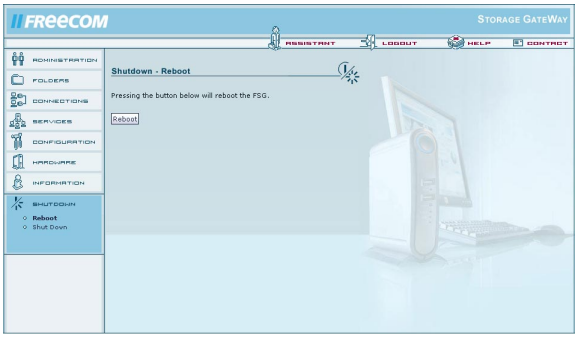
This screen allows you to reboot or shutdown the FSG. (You can then safely unplug the device from the power supply.)

Attention: Always shutdown the FSG before unplugging the power supply. If you do not do this, you may damage your drive or corrupt the system.

3.9.1 Reboot

Open Shutdown -> Reboot.

If you encounter any problems with the FSG, it may help if you restart the unit. Click 'Reboot' and the FSG restarts.

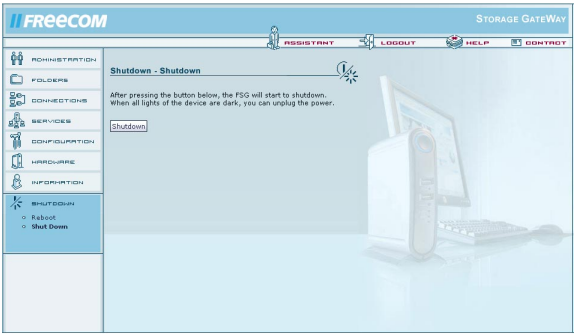


3.9.2 Shut Down

Open Shutdown -> Shut Down.

The FSG shuts down when you press the 'Shutdown' button. When all the lights on the device are off, you can unplug it from the power outlet. This may take a few seconds. Press the Power on button to turn the FSG back on.

Note: The LED ring stays on after the FSG has shut down.



Chapter 4: The Freecom Storage Gateway Wizard

The Freecom Storage Gateway Wizard helps you to locate each FSG in your network. When started, it displays all FSGs available in your network and helps you configure the FSG as a printer server or create network folders. You can also configure the basic settings and quickly find the configuration website using the FSG Wizard. You may also perform any of the functions of the FSG Wizard manually.

Note: The FSGW software only works with Windows.

4.1 Installation

Please place the Manual & Application CD on the tray. It contains user manuals and software, including the FSG Wizard. Once the CD is inserted, a window should appear automatically on the screen. If this does not happen, pleases proceed as follows:

1. Open your computer Desktop.
2. Double-click the CD drive containing the CD. The CD window should now open.

3. Click 'Install Software' -> 'FSG Wizard'. Follow the instructions for installing the software.
4. Start the FSG Wizard.

4.2 Features of the FSG Wizard

The preset password and login name for the FSG are:

Login Name: **admin**

Password: **admin**

4.2.1 Configure basic settings of your Freecom Storage Gateway

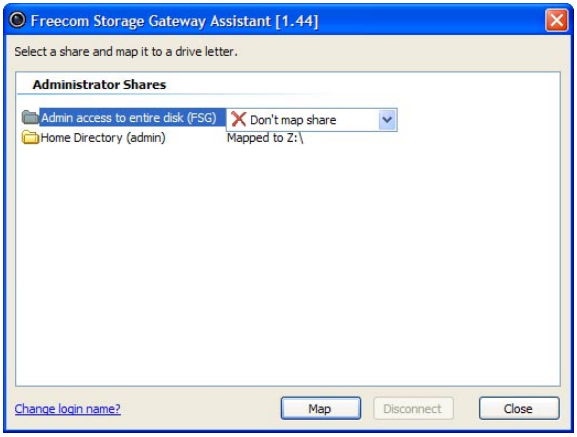
In this screen, you can set an IP address, subnet mask, device name and workgroup name for your FSG. With this information, it is easy to locate your FSG in the network without the wizard. To change the settings, you have to first enter the administrator password.

4.2.2 Accessing your FSG web interface

When you click this menu item, the web interface for your FSG opens in your default browser.

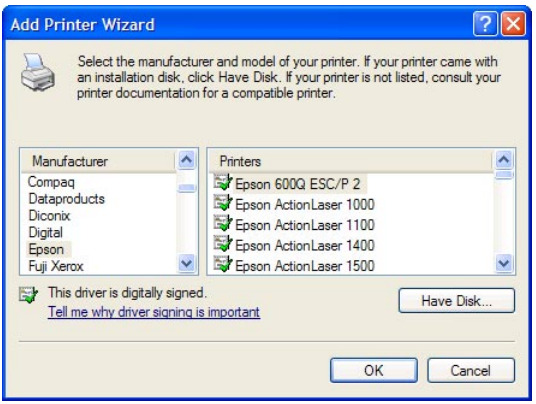
4.2.3 Adding and removing network drives

You can assign a drive letter to shared folders on your FSG. This allows you to access to the files in Windows more quickly.



4.2.4 Add a new printer

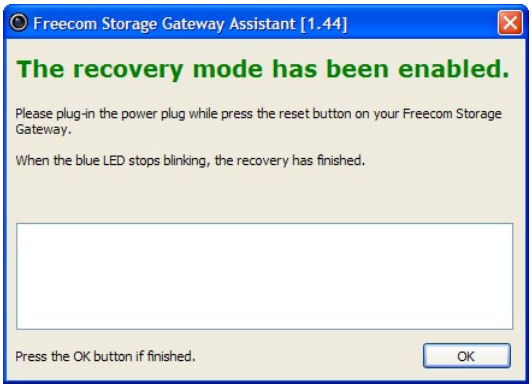
This windows allows you to configure any printer connected to your FSG on your local PC using Windows Printer Wizard.



Note: The attached printer has to be set up separately on each computer!

4.2.5 Start recovery procedure

This procedure can reset and repair an FSG to factory default settings if you cannot access your FSG anymore. Your user data will not be deleted!



To restore your settings, please proceed as follows:

a) Enable the Recovery mode by clicking 'Start the recovery procedure' in the Freecom Storage Gateway Wizard.

b) Turn the FSG off using 'Shutdown'.

c) Unplug the FSG's AC power pack.

d) Use a pointed object to carefully press the 'Reset' button. It is located next to the AC power slot on the back of the FSG.

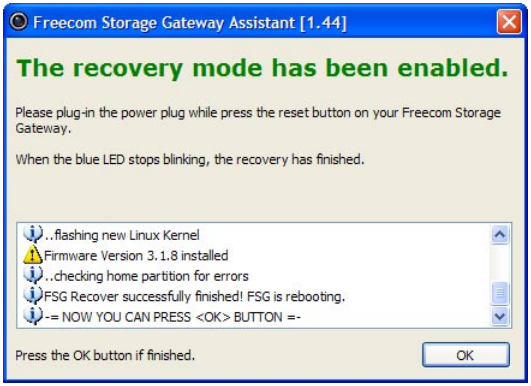
e) Keep the 'Reset' button pressed down and reattach the AC power supply.

f) Release the 'Reset' button.

g) The LED on the PWR button lights up, indicating that the Recovery mode is enabled. The device's LED flashes while the recovery process is taking place.

h) Once the LEDs stop flashing and the LED on the PWR button turns off, the recovery process is complete. A message window appears on screen, telling you that the recovery is finished.

i) Once it is complete, press OK in the Freecom Storage Gateway Wizard window.



Note: After recovery, all user data is still available on the FSG. To avoid problems, the administrator should backup all user data and format the hard disk. If an old configuration file was saved before, the administrator should load this configuration and afterwards copy the individual user data back to its folders.

4.2.6 Repeat search for available Freecom Storage Gateways

Click here to repeat the search for your FSG if it was not detected during the first search. Please make sure that your network is configured as described above in this manual and that all cables are properly attached.

Chapter 5: FSG in everyday use

5.1 WAN or internet connection setup

Next to using the FSG as a standalone router and NAS and connecting computers and switches and routers to the LAN ports, there is also the option of connecting the FSG WAN port to an existing router or straight to an internet modem.

5.1.1 Using the FSG behind a router

Note: When initially configuring the FSG, your computer needs to be connected to one of the LAN ports on this device.

Connecting the hardware

1. Connect a RJ45 cable to a LAN port on your router.
2. Plug the other end of the cable into the WAN port on the Freecom Storage Gateway.
3. Once the FSG is configured, you can connect the network PC to the FSG or your router.

FSG configuration

Using a fixed IP address Preparation

1. Check the 'DHCP' box under TCI/IP Settings in your computer's network settings. For more details, refer to Appendix B in this manual.
2. Connect your PC to the FSG.
3. Open the Internet browser and start the Configuration menu for the FSG (factory defaults: http://fsg or. http://192.168.1.1).
4. Open 'Connections' -> LAN' and select an IP address for the FSG.

To prevent conflicting IP addresses in your network, make sure the LAN IPs for your FSG and router are different.

5. Open 'Connection' -> 'WAN' and select 'Use fixed IP address'.

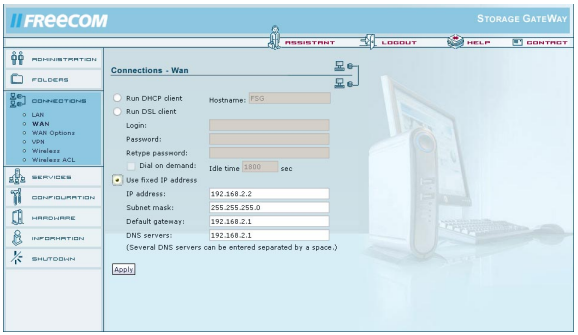
Use the following settings:

Specify the IP address: Enter an IP address that lies within the your router's address range; if the router's IP address is 192.168.2.1, enter 192.168.2.100 for your FSG.

This IP address allows you to access to the FSG from anywhere in your local network.

Subnet mask: Enter the subnet mask of your router (example: 255.255.255.0).

Standard Gateway: IP address of your router, e.g., 192.168.2.1.



Using the FSG behind a router when employing a fixed IP address

1. Open 'Services' -> 'File Server (CIFS)' and enable 'Open Windows File Sharing (CIFS/SBM) on the WAN port'.
2. If you want to access the FSG from outside the network (e.g., over the Internet) via HTTP (port 80) and FTP (port 21), you will need to forward these ports on your router to the IP address assigned by the router to the FSG. In this example, you are required to forward ports 21 and 80 to the IP address 192.168.2.100. For more details on forwarding ports, please refer to your router's manual.
3. Please make sure that 'Services' -> 'HTTP Server' -> 'Open HTTP server to the outside' and 'access for configuration pages from the outside" / 'FTP Server' 'open FTP server for the outside' are enabled in FSG's Configuration window.

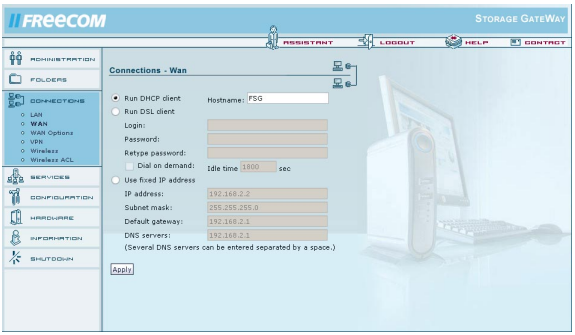
Note: The FSG DynDNS options do not function when the FSG is used behind a router. Please enable the router's DynDNS option.

Using DHCP

An alterative to using a fixed IP address is assigning your FSG a dynamic IP address through your router. You will need to enable your router's DHCP server before using the FSG as a DHCP client behind the router! For further details, please refer to your router's manual.

Before getting start

1. Check the 'DHCP' box under TCI/IP Settings in the network settings of your PC. For more details, refer to Appendix B in this manual.
2. Connect your PC to the FSG.
3. Open the Internet browser and start the Configuration menu for the FSG (fault defaults: http://fsg or http://192.168.1.1).
4. Go to 'Connections' -> 'WAN' and choose 'Run DHCP Client'. Click 'Apply'. Your FSG is now assigned an IP address by your router.



5. Enable the DHCP server on your router's Configuration window. For more information on this topic, please refer to your router's manual.
6. Connect the WAN port on your FSG to a LAN port on your router.

Using the FSG behind a router via DHCO

1. Open 'Information' -> 'Network'. You can view the IP address assigned by the router to your FSG under WAN Port -> IP address. If your router uses the IP address 192.168.2.1, the FSG IP address for example could be 192.168.2.100.
2. If you want to access the FSG from outside the network (e.g., over the Internet) via HTTP (port 80) and FTP (port 21), you will need to forward these ports on your router to the IP address assigned by the router to the FSG. In our example, you need to forward ports 21 and 80 to the IP address 192.168.2.100. For more details on forwarding ports, please refer to your router's manual.
3. Please make sure that 'Services' -> 'HTTP Server' -> 'Open HTTP server to the outside' and 'access for configuration pages from the outside" / 'FTP Server' 'open FTP server for the outside' are enabled in FSG's Configuration window.

Note: The FSG DynDNS options do not function when using the FSG behind a router. Please check your router's DynDNS box.

5.1.2 Using CIFS (Samba) over the Internet (behind a router)

CIFS (Samba) allows you to access the FSG over the Internet without any additional software. You can also map a folder on the FSG, i.e., add it to Windows. Mapped drives are network drives that can be used like normal folders.

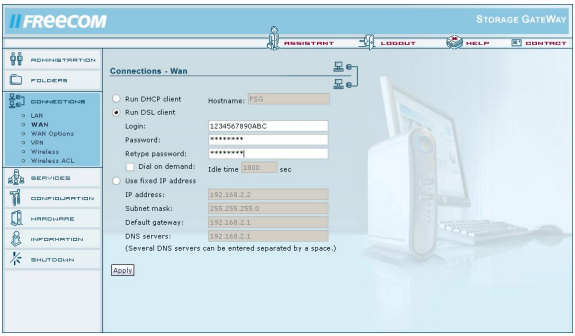
1. Open Services -> File Server (CIFS).
2. Check the box next to 'Open Windows File Sharing (CIFS/SMB) on the WAN port'.
3. Confirm by pressing 'Apply'.
4. Forward TCP ports 139 and 445 from the router to the LAN IP on your FSG. For more information on how to forward a port on your router to the FSG, please refer to your router's manual.
5. Your LAN is now configured for CIFS (Samba).

5.1.3 Connecting the FSG WAN port to a modem

To use the internet through your FSG, you will need to setup the FSG with the configuration information provided by your ISP. This information is described in detail in the "Getting on the internet" section of the "Before you begin" chapter.

To configure your FSG with this information, you should:

- Open the Web interface window of your FSG.
- Log on under 'admin' and administrator password.
- Click 'Connections' on the left-hand side of the window.
- Click 'WAN' on the left-hand side.
- If the IP data is prepared dynamically, check to make sure that 'Run DHCP Client' is enabled. The configuration is complete.
- If the IP data is not prepared dynamically, click the 'Run DSL Client' box.



- Enter the login data provided by your ISP.
- Click 'Apply'.
- Save your settings.
- To test the connection, start the Internet browser and see if you can access your Internet Favorites or check the Info window under WAN on the FSG configuration website to see whether your ISP has assigned you an IP address.

Note: It may take some time to establish the DSL connection to the ISP.

5.2 Dynamic DNS

A DynDNS entry allows you to access a computer using a dynamic IP address at any time under the same domain name. To do so, you first need to register with a DynDNS service. It updates the modified IP addresses and forwards this to the domain name. This enables you to be reached at one single domain name at any time even if your IP address changes ever so often.

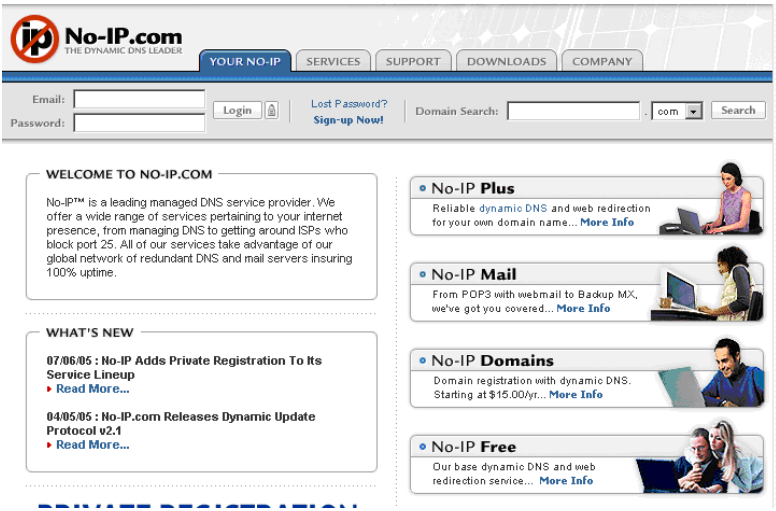
Your FSG supports three different DynDNS providers:

- www.dyndns.com
- www.dtdns.com
- www.no-ip.com

Creating a Dynamic DNS account (e.g., no-ip.com) and setting up a host

Note: You will need to register with a Dynamic DNS provider such as www.no-ip.com. Once you have registered at one of the providers, go to step 1.4.

1.1 To register at No-IP (requires a valid e-mail address), go to http://www.no-ip.com.



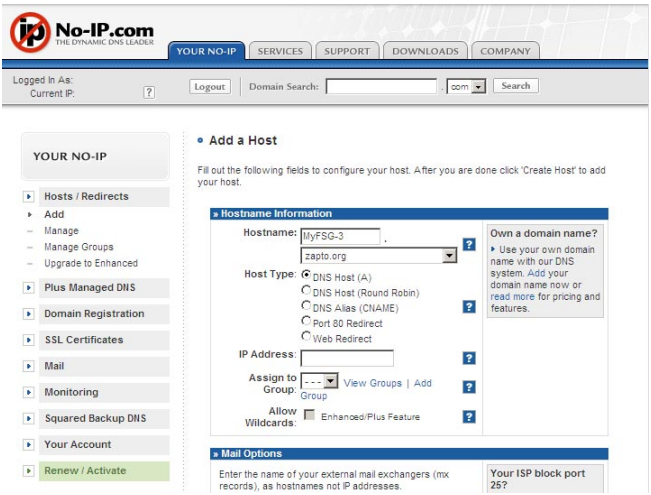
1.2 Press 'Sign-up now!' located next to the Login button. Enter the required information on the next page and click 'Sign-up now!'.

1.3 You will then receive an e-mail from No-IP, where you are asked to activate your account (This may take a few minutes.). Click the link in the e-mail to activate your account.

1.4 Log on to your No-IP account and create a host.

1.5 Adding a new host

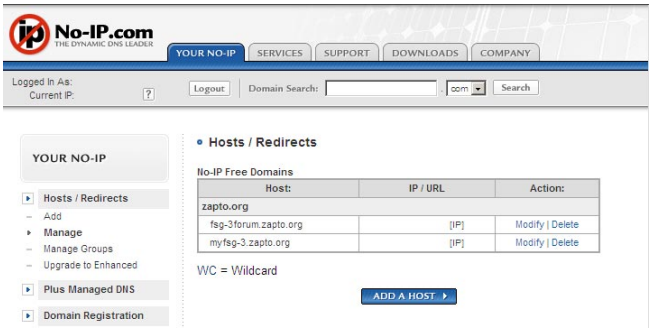
a. Select 'Host/Redirects -> 'Add' on the left section of the screen.



b. Enter the required hostname in the specified box and select a domain name such as 'zapto.org'. Choose a different host or domain name if the one you have entered is not available.

c. Click 'Create Host' and the new host has been added.

d. To view your account settings, click 'Host/Redirects' ->'Manage'.



Note: To set up a homepage on your FSG, you will require two hosts, one to access the FSG configuration and the other to access the homepage.

5.3 Setting up your own homepage on the FSG

You can set up one or more homepages on your FSG. They are accessed by entering the dynamic DNS address. Please follow these steps to set up a homepage on the FSG:

Configuring the FSG

Open 'Services' ->'Dynamic DNS'.

- Select 'no-ip.com' as the service.
- Enter one of the hosts created in chapter 12.2 (e.g., fsg- 3forum.zapto.org).

Note: This host allows you to access your configuration page from the outside via HTTP/ FTP/SSH.

- Username: the e-mail address used to register at no-ip.com.
- Password: Your no-ip password.
- Repeat password: Re-enter your no-ip password.

To access the Configuration pages from the outside, you will first need to enable 'Open HTTP Server to the outside' and 'Access for Configuration pages from the Outside' under 'Services' - 'HTTP Server'.

Setting up web front pages

- Add a new folder in the FSG configuration window (example: Homepage).
- Select 'New' under 'Services' -> 'HTTP Server'.
- Enter a name such as 'My Homepage'.
- Enter the second host created in step 1 in the field 'DNS Name' (example: MyFSG.zapto.org).

Note: You may use the same host as in step 2.1. Keep in mind that you can now only access your FSG configuration by entering the WAN IP address.

- Enter any port in 'Port'. (We recommend that you use port 80. If not, you will have to enter http://MyFSG.zapto.org:81/, with 81 indicating the port).
- As the 'Folder', select the one you created in step 3.1.
- Click 'Apply'. The HTTP now restarts.
- Create an index.html in the selected folder. This HTML page is opened whenever you access your host (e.g., http://MyFSG.zapto.org).

Web Front Page Aliases

Once your web front page has been set up, you can set aliases for your folders. Enable the check box for your web front page and click 'Properties'. Select 'New' on the 'Properties' screen.

Enter a name for your alias. You may choose any name.

- Please enter an abbreviation as the 'Alias' (e.g., mp3).
- Please enter the folder path in the field labeled 'Path' (e.g., files/test/user10/music/).

  You can now access this folder (for instance, files/test/user10/music/) using the alias (e.g., http:// MyFSG.zapto.org/mp3").

Note: If the path you enter ends with a slash ('/') (e.g., files/test/user10/music/), the user is required to enter the user, username and password whenever he accesses the alias address (e.g., http:// MyFSG.zapto.org/mp3). If the path does not end with a blank space (' ') (e.g., files/test/user10/music), the user is not be required to enter the username and password when accessing the alias address (e.g., http:// MyFSG.zapto.org/mp3).

Note: You can only use hosts from a provider. It is however possible to use multiple domains from one provider.

5.4 Setting up a printer

Windows: Installing a USB printer

To install a USB printer, connect the printer to one of the USB host ports on the FSG. Check to make sure the FSG is on. Now turn the printer on.

Installing using the Freecom Storage Gateway Wizard

1. Connect a USB printer to the FSG.
2. Open the FSG Configuration page and check whether the printer was detected under 'Information' -> 'USB'.
3. Start the Freecom Storage Gateway Wizard and click 'Add a new printer'. The FSGW automatically applies all settings. You only need to select the driver for your printer model.

Manual installation

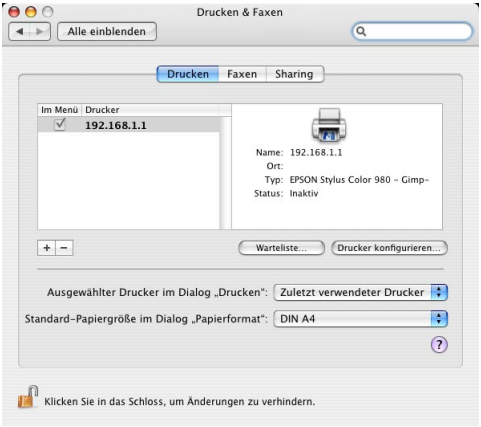
1. Connect a USB printer to the FSG.
2. Open the FSG Configuration page and check whether the printer was detected under 'Information' -> 'USB'.
3. Go to Start -> Settings -> Printer and faxes -> Add printer in Windows.
4. The print wizard starts. Click 'Next'.
5. Select 'Add local printer on this computer' and check the box next to 'Automatically detect and install my plug&play printer'. Click 'Next'.
6. Select the printer port in the next screen. Open 'Add new port' and select 'Standard TCP/IP port'. Click 'Next'.
7. The 'Add Standard TCI/IP port wizard' starts. Click 'Next' to continue. The 'Add port' window opens. Use the following settings: Printer name or IP address: FSG name or IP address of the FSG port name: 9100. Click 'Next'.
9. Now you need to enter the other port data. Set Device Type to: default (Generic Network Card) and click 'Next'. An overview of your settings is provided in the next screen. Click Finish.
10. To complete the installation, you now have to install the printer software. Select the software for your printer. If your printer is not contained in the list, hit 'Have Disk' and insert the drivers disk or CD for your printer.

Note: You can also use the Freecom Storage Gateway Wizard for quick installation of your printer in Windows. For detailed instructions on using the FSGW, please refer to chapter 4, 'The Freecom Storage Gateway Wizard'.

Mac OS X: Installing a USB printer

To install a USB printer, connect the printer to one of the USB host ports on the FSG. Check to make sure the FSG is on. Then turn the printer on.

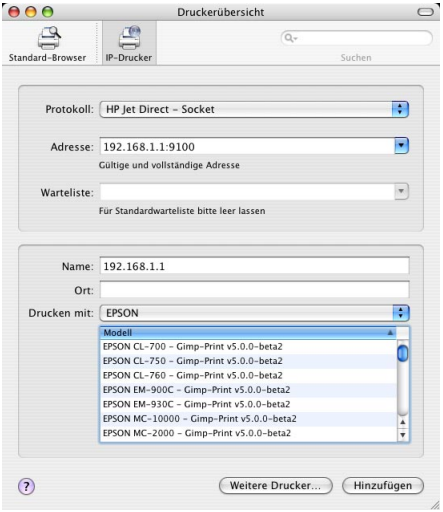
1. Connect a USB printer to the FSG.
2. Open the FSG Configuration page and check whether the printer was detected under 'Information' -> 'USB'.
3. Open 'System preferences' -> 'Printing & Faxing'.



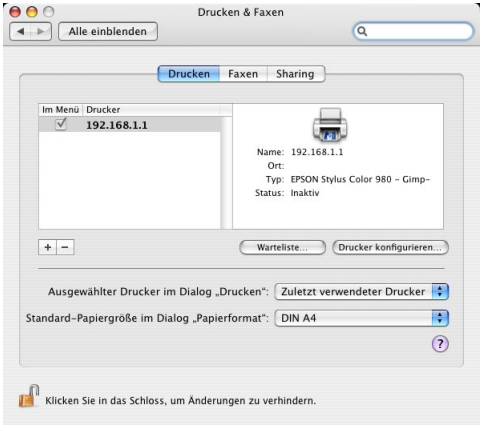
4. Click '+' to add a new printer.
5. The 'Printer Browser' opens. Select 'IP printer' as the printer type and select the following settings:

Protocol:	HP Jet Direct-Socket
Address:	192.168.1.1:9100 (replace 192.168.1.1 with the IP address that you set for your FSG)
Queue name:	You may leave this field blank.

A list of available printer drivers is now compiled.



6. You can enter additional information on the printer in the 'Name' and 'Location' fields.
7. Select the model of your printer under 'Print Using'. You may need to install the printer driver for your printer beforehand.
8. Click 'Add' to finish printer setup.



5.5 SSH Server

The SSH server is a secure terminal client that can be used to perform advanced configurations. Please use this only where absolutely necessary because each user with an account can also connect to the SSH server.

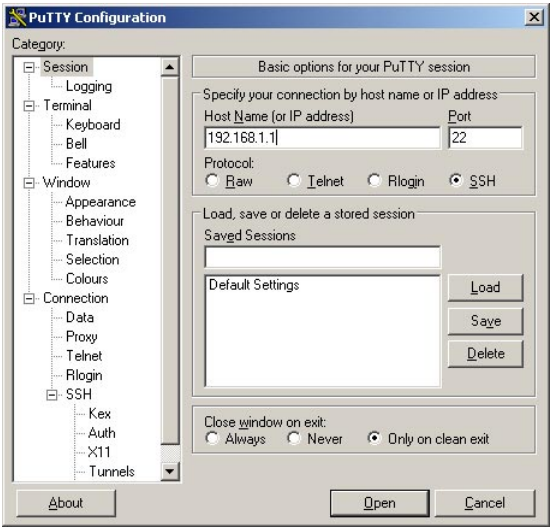
5.5.1 Starting the SSH server

Open 'Services' -> 'SSH Server' and enable 'Run SSH server'. If you also want to use the SSH server from the outside (Internet, router), enable 'Open SSH to the outside through the WAN port' and press 'Apply'.

Attention: Using an SSH server presents a security risk. Only do this if you trust the users!

5.5.2 Connecting with the SSH server for Windows

Install an SSH client (e.g., PuTTY) and start it. Enter your FSG's IP address/hostname:



With PuTTY, you only need to enter the IP address and hostname, and can leave all other settings unchanged. To connect, simply press 'Open':

Log on with the username and password.

Linux/Mac OS X

Open the console window or start 'Terminal' (Mac OS X). You now need to type in:

ssh FSG_IP –l admin

FSG_IP = IP address of your FSG (192.168.1.1, for instance). Now connect with the FSG's SSH server and sign in as admin. You can use the SSH server once you have entered the administrator password.

Sample SSH application

SSH allows you to instruct the FSG to download files from an FTP server. The file is then saved on the FSG without having to turn the PC on. This featureis particularly useful when downloading large files from slow FTP servers. The syntax for the 'ftpget' function is: ftpget -u <username> -p <password> <ftp server> local file path and name &

Example:

ftpget -u anonymous -p test@test.de ftp.ftp.com ftp.exe /pub/ test.exe &

User to Connect As:	anonymous
Password:	test@test.de
FTP server:	ftp.opera.com
Local file name:	ftp.exe —> name used to save the file on the FSG
Remotefilepathandname:	/pub/test.exe —> path and file name on FTP server & —> Continues download when PuTTY is closed.

5.6 Connecting External Drivers (USB, SATA)

5.6.1 USB

For more information on attached external USB mass storage devices, please refer to the section 'Information on the FSG configuration pages'.

Installing USB mass storage devices

To add more disk space to the FSG, plug a USB mass storage device into one of the USB host ports. Then turn on the external USB device. The disk space on theUSB device should appear as a shared folder. When using SMB (Windows File Sharing), it may take a few minutes until the Windows-based computer detects the new folder. If you are using a browser (HTML) to view your files, you can click Refresh. This shared folder can be accessed via FTP, HTML and SMB (Window File Sharing). The folder is configured with read and write privileges for all users located in the master directory (/). Once the device is attached, you can limit the user privileges. Please read the chapter on adding users and groups and on setting folder rights.

Attention: Optical drives such as DVD writers can only be used to read files and data.

Attention: When attaching a card reader, you need to insert the flash disk before connecting it to the FSG.

Power supply

All host ports can supply the USB-specific 500 mA current. If more power is required, please use the AC power supply that came with the external USB device.

File systems

The attached USB device has use in a file system format supported by the FSG. The supported file systems are:

FAT32

NTFS (read-only access)

ext2

ext3

reiserfs

HFS(+) (read-only access)

Note: To obtain full access to the external drive, we recommend that you use FAT32 when formatting the drive.

5.6.2 eSATA

Connection

To install a S-ATA external storage device, you must first shutdown the FSG. Go to the web interface and log in to the administration site. Go to the shutdown item of the Hardware menu and press shutdown. Wait till the FSG is shutdown and plug in the eS-ATA connector of the external device into the FSG eS-ATA port. Make sure the eS-ATA device is powered on and turn the FSG back on. The storage on the eS-ATA device should show up as a shared folder. This shared folder can be reached via FTP, HTML and SMB (Windows file sharing). The folder will be mounted with read and write rights for all in the root folder (/).

Filesystems

An attached S-ATA Disk must be formatted in a file system supported by the FSG. The supported file systems are:

FAT32

NTFS (read-only)

ext2

ext3

reiserfs

HFS(+) (read-only)

Remark: To have read/write access on the external disk, we recommend formatting the disk in FAT32 format.

5.7 Setting up Virtual Private Networks (VPNs)

A Virtual Private Network (VPN) is a computer network that uses a public network such as the Internet to transfer private data. VPN users can exchange data just like in an internal LAN. VPN are often used by companies as a way of providing access to the company network to staff when they are out of the office. The process involves the FSG establishing a VPN connection to the company's VPN gateway. Using this connection, the employee is then able to perform his duties as if he/she were working directly in the company's local area network.

Open Connections -> VPN -> ADD Connection in the main menu.

Status

You can enable or disable the VPN connection at any time here.

Name

Please enter any name of your choosing for the connection here.

Remote Host IP

In this field, please type in the IP address of the VPN routers that you wish to connect to (you need to have an account on this router).

Remote Network

Enter the IP address and the network mask that you want to access. Example: 192.168.1.0/24. The '0' at the end of the IP address signifies that you can reach any PC in the network under the IP addresses 192.168.1.1 – 192.168.1.254. /24 indicates that this is a network mask 255.255.255.0. If the network you are attempting to access contains several subnets with the net mask 255.255.252.0, please enter /22 in place of /24.

ESP Encryption

This is where you set the encryption protocols. You can keep the default settings, although they have to be supported by the remote machine.

ESP Encryption 3Des

Triple DES (3DES) is an advanced version of the Data Encryption Standard (DES). The old DES only used key lengths of up to 56 bits. 3DES on the other hand uses three encryption cycles and two or three keys. By using three keys, an actual key length of 112 bits is provided.

MD5

MD5 sums are used by PGP and other programs to check the integrity of files. This involves comparing the file's current MD5 sum with an accepted sum from earlier. This allows the system to determine whether the file has been changed or is corrupt.

SHA1

Secure Hash Algorithm (SHA) is the term used to describe a group of standardized cryptographic hash functions.

Working together with the National Security Agency, the National Institute of Standards and Technology (NIST) developed a secure hash function for signing as part of the Digital Signature Algorithms (DSA) for the Digital Signature Standard (DSS). It was released in 1994. The name given to it was the Secure Hash Standard (SHS). It specifies the Secure Hash Algorithm (SHA), with a hash value of 160 bits for messages up to 264 bits in size. The algorithm shares a similar structure with MD4, designed by Ronald L. Rivest. There are two versions of the Secure Hash Algorithm: SHA0 and SHA1. They differ in the number of cycles passed through when generating the hash value.

Pre-Shared Key

Similar to a password. Has to be the same on both VPN routers (FSG and remote VPN router).

Operation

1. Establish connection - Allows you to establish a connection with another VPN router.
2. Listen Only - Allows you to accept a connection from another router.

Alive Ping IP

You can enter the router's IP address used in establishing a connection in this field. This involves sending a ping at set intervals to ensure that connection is not cut when no activity is registered over a long period of time.

5.8 Setting up an FSG Mail Server

An e-mail server, or simply mail server, handles e-mails. It is responsible for receiving, sending, saving or forwarding e-mails.

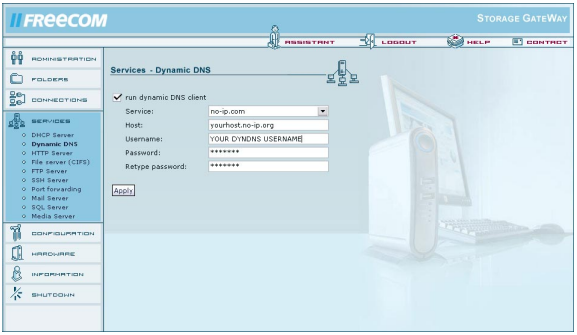
Note: In the name of spam protection, some freemail providers refuse to accept e-mails received from dynamic DNS hostnames. Please keep this in mind when sending e-mails!

Configuring the FSG

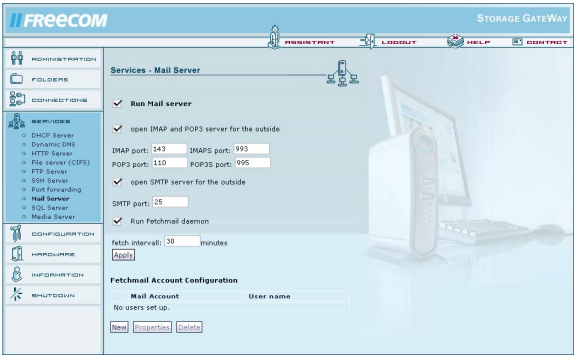
The FSG mail server supports **POP3** (Post Office Protocol Version 3) and **IMAP** (Internet Message Access Protocol) for retrieving and **SMTP** (Simple Mail Transfer Protocol) for sending e-mails.

POP3	Communications protocol for retrieving e-mails using an e-mail client. POP3 allows the user to retrieve and delete e-mails on the server. A permanent connection to the POP3 mail server is not required. The fetched e-mails are stored locally and available offline.
IMAP	The IMAP protocol allows the user to access and manage e-mails directly on the server using an e-mail client. Unlike the POP3 protocol, the e-mails generally remain on the server and are only transferred to the client as required. In other words, you need an Internet connection to read the e-mails. IMAP provides detailed access control to mailboxes as POP3. **Note: Many freemail providers only support POP3!**
SMTP	The SMTP protocol is used to exchange e-mails within computer networks. SMTP is mostly used to send and forward e-mails.

Set up a Dynamic client under Services -> Dynamic DNS if you have not already done so. Your e-mail address corresponds to the hostname that you set earlier, e.g., xxx@yourhost.no-ip.org (xxx is a user that you previously added on the FSG; yourhost.no-ip is the hostname that you selected at the Dynamic DNS provider).



Open Services -> Mail Server and start the mail server by enabling 'Run Mail Server'. Click 'Apply' to start the mail server. The mail server is now ready for use in the internal network.



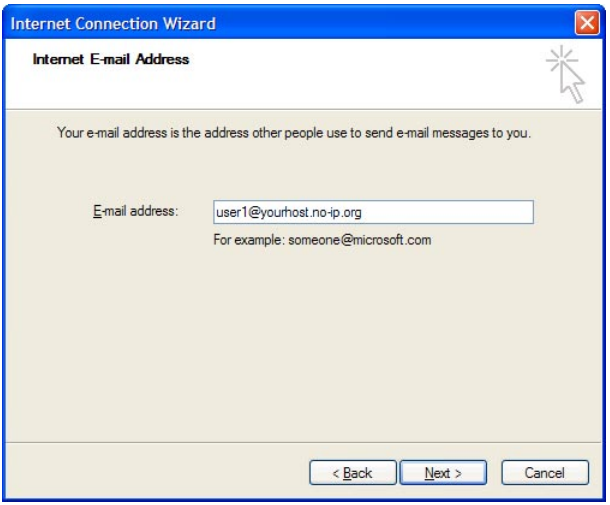
To receive e-mails from the outside (Internet), you have to enabled 'Open IMAP and POP3 Server for the outside'. You may now change the preset default ports. This is however generally not required. To send e-mails to accounts outside of your network, you need to enable 'Open SMTP Server for the outside'. You generally do not have to change the default port (25).

Configuring an e-mail client in Outlook Express

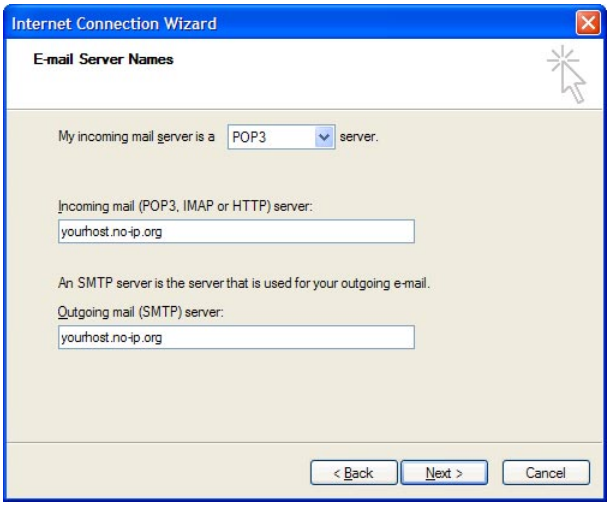
You require an e-mail client to retrieve and read e-mails. Using the e-mail client Outlook Express, already built-in to the Windows operating system, we will demonstrate which changes you have to make to the configuration settings. Start Outlook Express. If you have not already set up an e-mail account, the Configuration wizard will open:

1. Enter your name as you would like it to appear in the Sender field. Click 'Next'.

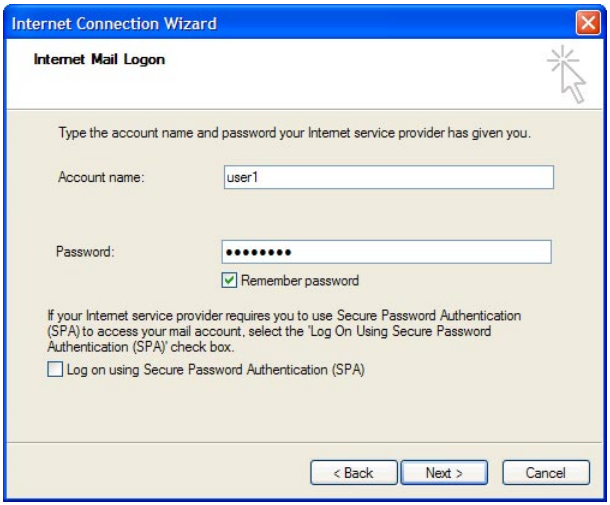
2. Enter your e-mail address here. This is a combination of your username on the FSG and the dynamic DNS host you created earlier. The FSG administrator has for example the e-mail address admin@yourhost.no.ip.org (yourhost.no-ip is the dynamic DNS hosthame that you entered earlier). Click "Next".



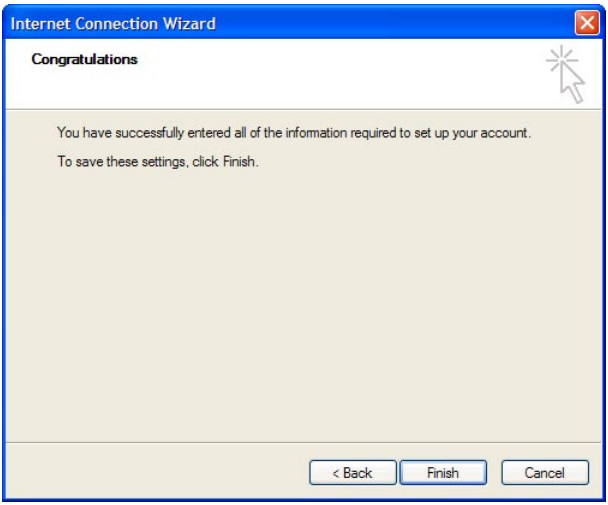
3. Select whether the e-mails are retrieved via the POP3 or IMAP server and enter your dynamic DNS hostname under Server (e.g., yourhost.no-up). Please enter the same dynamic DNS host for both the POP3 and the SMTP servers. Click "Next".



4. Then enter your login data (account name and password). Click "Next".



5. To complete the configuration, please click 'Finish'.



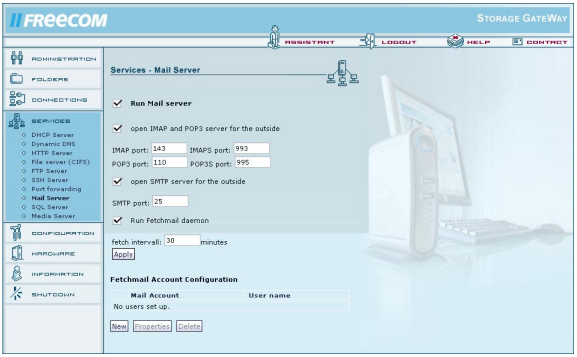
6. To test your configuration, you can now send an e-mail to yourself and to someone else.

Using Fetchmail

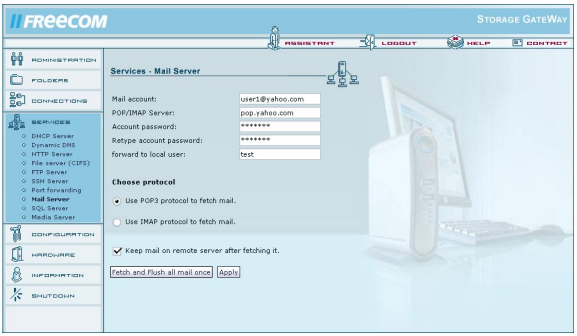
Fetchmail retrieves e-mails from an e-mail server. It retrieves the e-mails and transfers them to the local e-mail system. Fetchmail is mostly used to check several e-mail servers one by one. The e-mails are then forwarded to the mail folder of the recipient.

Note: You cannot use Fetchmail unless the mail server is enabled!

1. In the mail server configuration screen, click 'New' under 'Fetchmail Account Configuration'.



2. An input screen opens where your can type in the Fetchmail information.



3. Enter your details for the e-mail account that Fetchmail checks for new e-mails.

Mail account:	E-mail address that is checked for new e-mails.
POP/IMAP server:	The server address of the e-mail server (POP3 or IMAP)
Account password:	Password for e-mail account
Retype Account password:	Re-enter the e-mail account password.
Forward to local user:	FSG user who will receive the e-mails.

4. Under 'Choose Protocol', you need to select a protocol: POP3 or IMAP.

Note: Freemail providers generally use the POP3 protocol.

5. To leave the e-mails on the mail server after retrieving them, enable 'Keep mail on remove server after fetching it'.

6. Click 'Apply' to finish set-up.

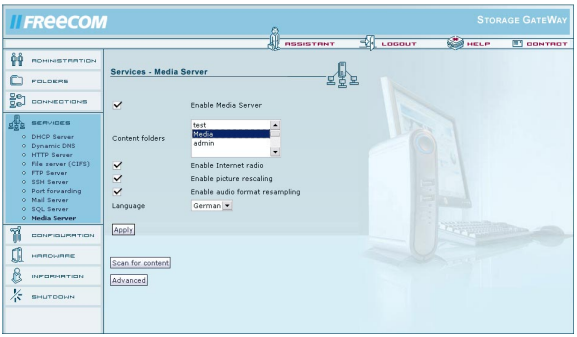
Note: 'Fetch and Flush all mail once' is only available if 'Keep mail on remote server after fetching it' is enabled!

You may set up as many accounts as you need and access them via Fetchmail. To add new accounts, repeat the steps described above.

5.9 Using the media server

1. Open 'Services' -> 'Media Server'.
2. Activate the Media Server by checking 'Enable Media Server'.
3. You can view all available FSG folders under 'Content Folders'. Select one or more folders. To select more than one folder, keep the CTRL key pressed while making your selections.
4. Click 'Apply' and then 'Scan for Content'. The selected folders are now scanned for multimedia files.
5. Click 'Advanced'. You will see how many files were located under 'Multimedia files found'.

Note: You should not change any of the settings under 'Advanced' unless you are an experienced user.



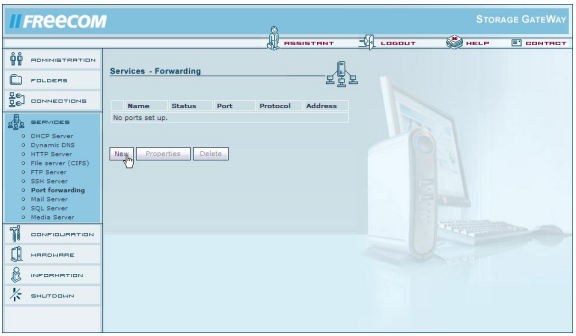
A list of media formats supported by the media server is located in Appendix D, 'Media Formats Supported by Media Server'.

5.10 Port Forwarding

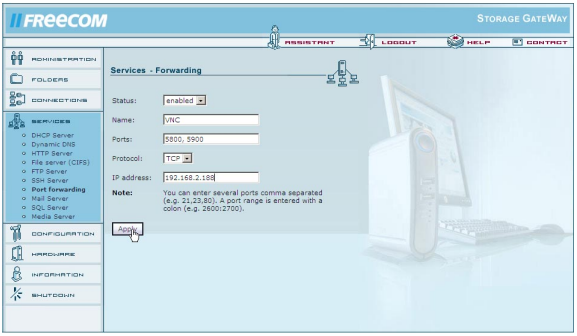
Port forwarding allows you to forward ports from clients on the local network to any port(s) on the FSG that you select. This makes it possible to access services of the local area network from other networks such as the Internet. Services on certain clients can thus act as servers as they can now be reached via preset ports that no one else is using.

Example using the remote tool VNC

Click 'Services' -> Port Forwarding on the overview. To add a new forwarding, click 'New'.



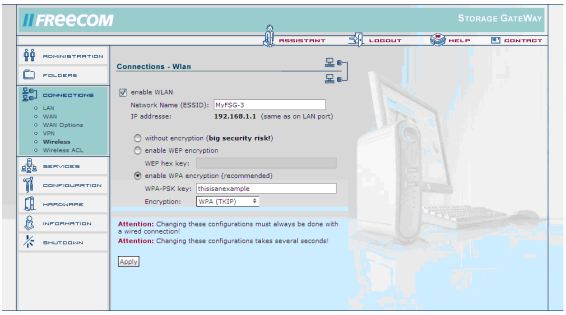
You may choose any name for the port sharing. You can either share individual ports (separated by a comma) (see example) or set an entire range of ports by inserting a ':' between each of them. You can set the protocol in the drop-down menu 'Protocol' and the client IP address of the port(s) in your local area network under 'IP address. VNC requires ports 5800 and 5900. Enter these two ports as seen in the illustration below. Select the TCP protocol and enter the IP address of the computer where the ports are forwarded. Then press 'Apply'.



5.11 WLAN in Everyday Use

To use the WLAN function on your FSG, please select which method of encryption used by device that you want to attach to the FSG.

Setting up a WAP – TKIP connection



1. Go to 'Connections' and then click 'Wireless' on the web interface. This window contains the main settings options for WLAN.
2. Enter the name used to identify your FSG in the network under 'Network Name(ESSID)'. You may choose any name. In this example, we are using 'MyFSG'.
3. Check the box labeled 'enable WPA encryption (recommended)'.
4. Enter one of the authentication keys selected by you under 'WPA-PSK key'. This key has to be at least eight and no more than 63 characters in length. Jot down the key that you just typed in. It needs to be entered on all of the devices that will connect to your FSG via WLAN.

In this example, we are using 'thisisanexample'.

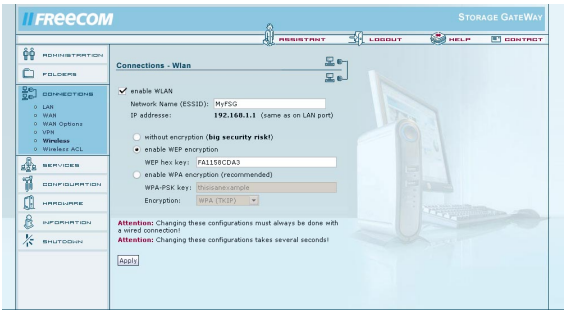
Please do not use this code word for security reasons!

5. Select 'WPA TKIP' under 'Encryption'.
6. Confirm your settings by pressing 'Apply'.

Your FSG is now configured for WLAN using WPA TKIP.

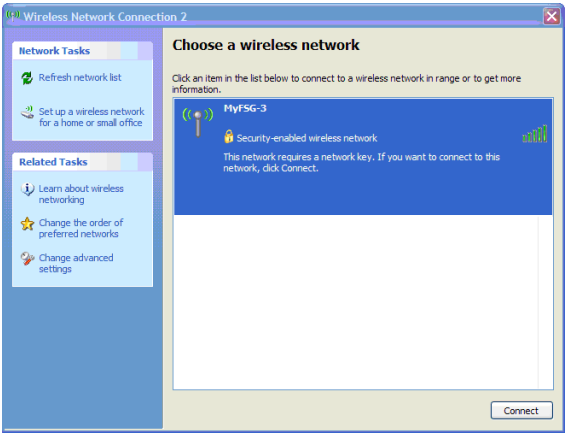
Example: Setting up a WEP connection

1. Go to 'Connections' and then click 'Wireless' on the web interface. This window contains the main settings options for WLAN.
2. Enter the name used to identify your FSG in the network under 'Network Name(ESSID)'. You may choose any name. In the example provided here, we are using 'My-FSG'.
3. Select 'enable WEP encryption' (refer to illustration) and enter any authentication key of your choosing under 'WEP' 'hex key'. This key has to contain either 10 or 26 characters. Jot down the key that you just typed in. It needs to be entered on all of the devices that will connect with your FSG via WLAN.



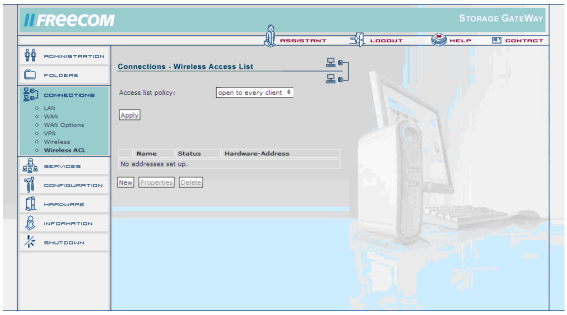
In this example, we are using the key 'FA1158CDA3'. For security reason, you should not use this key. Please use WEP only if your WLAN devices do not support WPA. The WEP standard is outdated and not secure!

5.12 Establishing a WLAN connection to your FSG

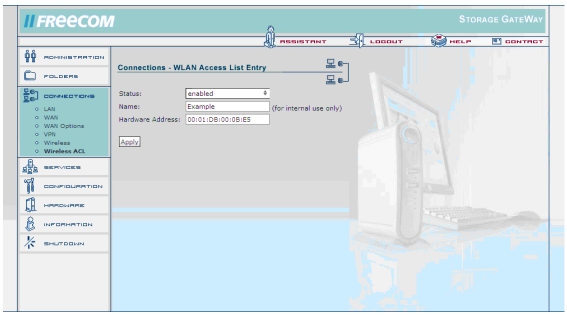


1. Click 'Start', 'Settings', 'Control Panel'.
2 Click the 'Network Connections' icons in the Control Panel window.
3. Double-click 'Wireless Network Connections' in the window that appears.
4. A new window opens and displays the available wireless networks.
5. Double-click on the name you selected for your FSG (set under 'Network Name(ESSIUD)). In this example, it is MyFSG.
6. A dialog window appear on the screen where you are requested to enter the authentication key selected in step 4 (Setting up a WAP TPIK connection) twice.
7. Click OK. You computer then establishes a connection with the FSG.

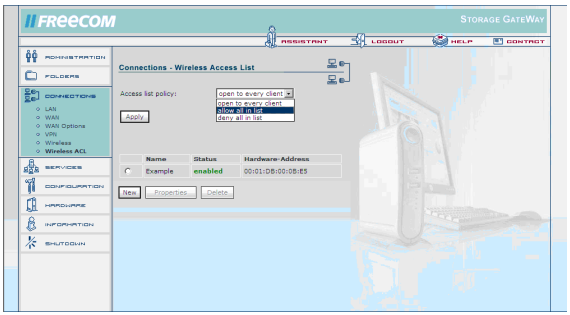
Example: Setting up a wireless ACL filter



1. Go to 'Wireless ACL'. Click 'New' to add devices to enabled or restricted.



2. On this page, you can set enabled/restricted by checking or unchecking 'enabled' / 'disabled'. Enter any name in the Name field. Click 'Apply' to confirm your entries. In this case, we are using 'Example'.



3. You are now back at the Wireless ACL screen, where you can select either 'allow all in list' or 'deny all in list' for the connection. Click 'Apply' to accept the final settings.

Appendix A: CE, FCC and other certifications

CE

EN 55 022 Declaration of Conformance. This is to certify that the Freecom Storage Gateway is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

FCC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Appendix B: Preparing LAN for use with the FSG

This appendix provides a description of how to prepare your computer network for connecting with the FSG and the Internet.

Preparing the computer for connection to the FSG

To connect to the FSG, you have to install TCP/IP (Transmission Control Protocol/ Internet Protocol) on each of your network computers and select the required network protocol. If a network interface card (NIC) is already installed on your PC, then TCP/IP is probably also already installed.

Configuring Windows 98 SE and Windows Me to work with the FSG

To use your network and FSG, you will need to manually install TCP/IP and configure it on each computer in the network. Have your Windows CD handy before you begin as you may need it when installing TCP/IP.

Installing the required network components

To install or scan for the components required for IP network operation:

1. Click 'Start' - 'Settings' - 'Control Panel' on your Windows taskbar.
2. Double-click the Network icon. The Network form contains a list of installed components.

You need to make sure that an Ethernet adapter (NIC), the TCP/IP protocol and the Client for Microsoft Networks are installed. You do not need to remove any of the other components displayed in the Network Components window.

Installing an Ethernet adapters (NIC)

a. Click the 'Add' button.
b. Select an adapter and click 'Add'.
c. Select the manufacturer and model of the Ethernet adapter and then click 'OK'.

Installing TCP/IP:

a. Click the 'Add' button.
b. Select Protocol and click 'Add'.
c. Select Microsoft.
d. Select TCP/IP and then click 'OK'.

Installing Client for Microsoft Networks:

a. Click the 'Add' button.
b. Select Client and click 'Add'.
c. Select Microsoft.
d. Select Client for Microsoft Networks and then click 'OK'. Please restart your PC in

Obtain your TCI/IP configuration via DHCP

Once the TCP/IP protocol has been installed, you need to add certain information on each computer to ensure that other network devices can be accessed. The FSG is preconfigured to automatically forward this information to all computers connected to its LAN ports. The computers can obtain this information from FSG's internal DHCP server. To use DHCP with the recommended default addresses, please follow the instructions step by step:

1. Start the FSG and wait until it boots. The LED ring lights up once the boot process is complete. (This may take up to 30 seconds.) Connect all computers to the LAN port on the FSG.
2. Open the Network Control Panel on each of the attached computers and go to the 'Configuration' tab.
3. Select TCT/IP->(your Ethernet adapter) from the list of network components and click 'Properties'.
4. Go to 'Obtain an IP address automatically' on the IP Address tab.
5. Open the 'Gateway' tab.
6. If any Gateways are listed, delete them.
7. Click 'OK'.
8. Restart your computer. Repeat steps 2 - 8 on each computer in your network.

Selecting the type of Internet access

1. Click the 'Start' button on the Windows taskbar, go to 'Settings' and then click 'Control Panel'.
2. Double-click the 'Internet Options' icon.
3. Select 'I want to set up my Internet connection manually' or 'I want to connect through a Local Area Network' and click 'Next' to continue.
4. Select 'I want to connect through a Local Area Network' and then click 'Next' to continue.
5. Uncheck all boxes on the LAN Internet Configuration screen and then click 'Next'.
6. Follow all the instructions provided by the Wizard.

Check the TCP/IP properties.

Once your PC has been configured and restarted, you can check the TCP/IP configuration using the utility program winipcfg.exe:

1. Click 'Start' in the Windows taskbar and then press 'Run'.
2. Enter 'winipcfg' and then click 'OK'. The program winipcfg lists among other things your IP address, subnet mask and standard Gateway.
3. Choose your Ethernet adapter from the drop-down menu. The window is refreshed and shows your settings. These should look like this if you are using the default settings for TCP/IP recommended by Freecom:
4. The IP is between 192.168.1.2 and 192.168.1.254.
5. The subnet mask is 255.255.255.0.
6. The standard Gateway is 192.168.1.1.

Configuring Windows XP, NT or 2000 to work with the FSG

To use your network and FSG, you may need to manually install TCP/IP and configure it on every computer in the network. Have your Windows CD at hand before you begin as you may need it when installing TCP/IP.

Installing or scanning Windows

Network components

You need to make sure that an Ethernet adapter (NIC), the TCP/IP protocol and the Client for Microsoft Networks are installed. You do not need to remove any of the other components displayed in the Network Components window. If you need to install the adapter, please refer to the instruction manual that came with the adapter on how to install the device. To install or scan for the other components:

1. Click the 'Start' button on the Windows taskbar, go to 'Settings' and then click 'Control Panel'.
2. Double-click the Network icon and Dial-up Connection (these may also be called Network Connections or Connect Using on the Mac).
3. If your computer has an Ethernet adapter, you should see an entry for a Local Area Connection. Double-click this entry and open the 'Properties' tab.
4. Open the 'General' tab.
5. Check to make sure that 'Client for Microsoft ´Networks' and 'Internet Protocol (TCP/IP)' are displayed on this screen. If they are not, go to 'Install' and add them.

6. Select 'Internet Protocol (TCP/IP), click 'Properties' and check to make sure that 'Obtain an IP address automatically' is enabled.
7. Click 'OK' and close all windows for network and dial-up connections.
8. Make sure that the computer is connected to the FSG and check the TCP/IP properties (see below). If you notice any problems, you can restart the computer.

Check the TCP/IP properties.

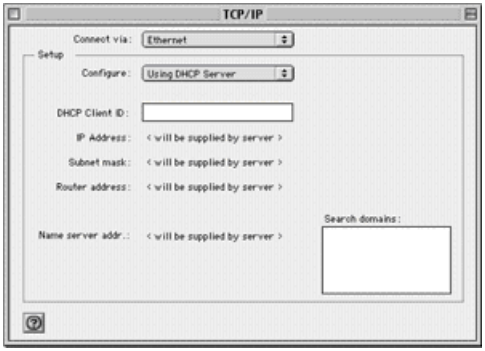
To check the computer's TCP/IP configuration:

1. Click 'Start' in the Windows taskbar and then press 'Run'. The 'Run' screen opens.
2. Enter 'cmd' and then click 'OK'. A command window appears on the screen.
3. Type in ipconfig /all. Your configuration details are displayed and should be as follows if you are using the default settings for TCP/IP recommended by Freecom:
4. The IP is between 192.168.1.2 and 192.168.1.254.
5. The subnet mask is 255.255.255.0.
6. The standard Gateway is 192.168.1.1.
7. Type in exit.

MacOS 8.6 or 9.x

With Macintosh OS 7 and higher, TCP/IP comes preinstalled on the Macintosh. To use DHCP, you need to configure TCP/IP on each Macintosh in the network.

1. Open Apple's 'System Preferences' and hit 'TCP/IP'. System Preferences TCP/IP opens:



2. In the 'Connect via' field, select the Macintosh Ethernet interface.

3. Select 'Use a DHCP server' in the 'Configure' field. You may leave the DHCPClient ID field blank.
4. Close System Preferences-TCP/IP.
5. Repeat these steps on each Macintosh in your network.

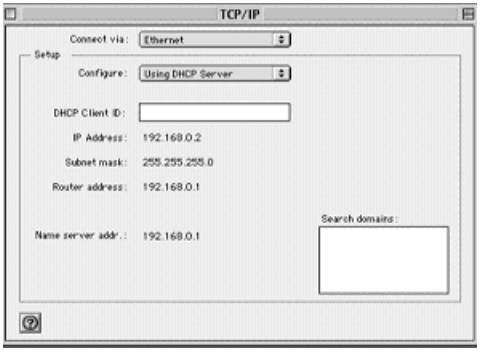
MacOS X

With Macintosh OS 7 and higher, TCP/IP comes preinstalled on the Macintosh. To use DHCP, you need to configure TCP/IP on each Macintosh in the network.

1. Open 'System Preferences' and then 'Network'.
2. If it has not already been selected, click 'Built-in Ethernet' from the configuration list.
3. If this has not been selected, click 'Use DHCP' on the TCP/IP tab.
4. Hit 'Save'.

Check the TCP/IP properties (Macintosh).

Once your Macintosh has been configured and restarted, you can check the TCP/IP configuration by once again opening TCP/IP System Preferences. Open Apple's 'System Preferences' and hit 'TCP/IP'.



The overview is refreshed and shows your settings. These should look like this if you are using the default settings for TCP/IP recommended by Freecom:

1. The IP is between 192.168.1.2 and 192.168.1.254.
2. The subnet mask is 255.255.255.0.
3. The router address is 192.168.1.1.

If different values are displayed, restart your Mac. It may be the case that you need to enable another option in the 'Configuration' settings and then return to 'Use a DHCP server'.

Accessing the Internet

If you do not have an Internet account, but still need to access the Internet, you have to sign an agreement for a Single User Internet Access account with an Internet service provider. You may use either DSL or cable DSL. You will require a separate modem based on the type of Internet account you have. These modems are used to access the internet and are usually provider by your ISP. You can then connect the WAN port on the FSG directly to a modem. To install the FSG, you need certain information from your ISP. Please make sure you have this information available to you. This user's manual provides detailed instructions on how to configure an Internet account on the FSG.

Information on the Internet configuration

Your ISP will supply you with details on TCP/IP configuration (such as IP address, subnet mask and standard Gateway) for a Single User Internet Account as well as information on VPI and VCI multiplexing. Your ISP will provide you with other login data such as the username and password should you require a PPoE or PPPoA protocol. In most accounts, the lion's share of configuration data is obtained dynamically when the computer is booted the first time while connecting to the ISP. You therefore do not need to know this dynamic data.

FSG acts as a single computer in order to enable multiple computers to use the Internet connection at the same time, your . At this stage, you need to configure it by adding the TCP/IP data typically required by each of the computers. If WAN port on the FSG is connected to the modem, the FSG is recognized by the ISP as one single computer. The gateway allows the computers in the local area network to access the Internet through the broadband modem using a Single User Account. The method used to access the FSG is referred to as Network Address Translation (NAT), or IP masquerading.

Login protocols

Some ISPs require a special login protocol, where you are required to enter a login name and password to access the Internet. If you already log on to your Internet account using a program such as WinPOET or EnterNet, your account will use PPP via the Ethernet (PPPoE). When configuring your FSG, you have to enter your login name and password in the configuration window. Once you have configured your network and FSG, the FSG automatically logs in for you (where required) and you therefore no longer need to sign in from your computer. You do not need to uninstall the login program.

Account data

If the values are not obtained dynamically from the ISP, you should provide your ISP with the following basic information on your account:

1. An IP address and subnet mask
2. A gateway IP address (the address of the ISP router)
3. One or more Domain Name Server (DNS) IP addresses
4. Host name and domain suffix

The full server name for your account could look something like this: mail.xxx.yyy.com. (In this example, the domain suffix is xxx.yyy.com.= If any of this information is obtained from your ISP dynamically, your gateway receives it automatically. If a service technician from the ISP configured your computer while installing the broadband modem or if you have configured it following the instructions provided by your ISP, you will need to copy the configuration data from the 'Properties' window of the Network TCP/IP on your computer (or the TCP/IP System Preferences on your Macintosh) before reconfiguring your computer for use with the FSG. This process is described below.

Locating the ISP configuration data (Windows)

If your computer was connected directly to the modem for accessing the Internet, you may have to obtain the configuration data from your computer for use in configuring the FSG. If your ISP has supplied this information in print-out form or if it obtains the configuration data dynamically, you will not require this information. To obtain the information needed to configure the FSG for Internet access:

1. Click the 'Start' button on the Windows taskbar, go to 'Settings' and then click 'Control Panel'.
2. Double-click the Network icon. The 'Network' form appears on the screen with a list of installed components.
3. Select 'TCP/IP and then click 'Properties'. The 'TCP/IP' dialog window opens.
4. Open the 'IP Address' tab. If both an IP address and subnet mask are displayed, write this information down on a piece of paper. Now click 'Obtain an IP address automatically'. If no address is provided, your account will use an IP address obtained dynamically and you will not require any additional information. Close the window and continue with the installation of your computer and FSG.

5. Open the 'Gateway' tab. If an IP address is shown under 'Installed Gateways', write this down. This is the IP's gateway address. Select an address and click 'Remove' to delete the gateway address.
6. Open the 'DNS Configuration' tab. If several DNS server addresses are displayed, write these down. If any information is shown in 'Host' or 'Domain' information fields, you should also jot this down. Click 'Disable DNS'.
7. Click 'OK' to save your settings and close the 'TCP/IP Properties' window. You now return back to the 'Network' window.
8. Click 'OK'.

Obtaining the ISP configuration data (Macintosh)

If your computer was connected directly to the modem in order to access the Internet, you may have to get the configuration data from your computer for use in configuring the FSG. If your ISP has supplied this information in print-out form or if it obtains the configuration data dynamically, you will not require this information. To obtain the information needed to configure the Gateway to access the Internet:

1. Open Apple's 'System Preferences' and hit 'TCP/IP'. System Preferences - 'TCP/IP' opens and displays a list of configuration settings. If 'Configure' is set to 'Use a DHCP server', your account uses an IP addressed obtained dynamically and you do not require any additional information. Please close the window and proceed with the installation of your computer and FSG.
2. If both an IP address and a subnet mask are displayed, write this information down on a piece of paper.
3. If an IP address is shown under 'Router Address', write this down. This is the IP's gateway address.
4. If several name server addresses are displayed, write these down. These are your ISP's DNS addresses.
5. If any information is displayed in the 'Domain Search' information field, you should also jot this down.
6. Change settings under 'Configure' to 'Use a DHCP server'.
7. Close TCP/IP-System Preferences.

Restart the network.

Once your computer is configured to work with the FSG, you need to reset the network so that the devices can properly communicate with each other.

1. Turn off the FSG if it is on. Turn it back on and wait until it has rebooted. (This may take up to 30 seconds.)
2. Restart all computers attached to the FSG.

Ready to configure

Once all computers are set to TCP/IP network mode and connected to the local area network of your FSG, you can access the FSG and configure it.

Appendix C: Networks and Routing Basics

This chapter provides an overview of IP networks, routing, and firewalls. This is by no means a complete overview! If you are looking for more information, you can use your favorite search engine to find information on the internet about the internet. Suffice to say, there is plenty.

Basic Router Concepts

Even though the amount of bandwidth in your local area network (LAN) can be provided easily and relatively inexpensively, the price of the connection to the internet is much higher. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. To use this WAN link efficiently, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router splits the information meant for your network and meant for other networks, so the available bandwidth is used efficiently. The router sends data based on network layer information in the data and on routing tables maintained by the router. The routing tables are built by gathering and exchanging information with other routers in the network. The router builds up a logical picture of the overall network. Using this information, the router chooses the best path for forwarding network traffic. Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support.

Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

IP Addresses and the Internet

For a computer to communicate with other computers and Web servers on the Internet, it must have a unique IP address. An IP address (IP stands for Internet Protocol) is a unique number that identifies the location of your computer on a network.

Basically, it works like your street address — as a way to find out exactly where you are and deliver information to you. The IP address is written as 4 numbers between 0 and 255, such as "192.168.0.12".

This serves the same basic function as a street address. It helps you find out where you currently are, while also providing other information. The IP address consists of four numbers between 0 and 255 (e.g., 192.168.0.12).

Domain Name Server

The computer address is difficult to read, which is why a second system is used in the Internet by the name of DNS (Domain Name Server). This translates human-readable names such as www.sharemydisk.com into computer readable names like 82.161.11.206. Each Internet user must have an IP address. You do not need the human-readable name, but it is quite useful if you want other users to find you. A few examples of this include: if you operate a web server or if you want to show your friends images stored on your computer. Many large companies such as ISPs maintain their own DNS server and let their customers use the server to search for addresses.

Internet address classes

The Internet Assigned Numbers Authority (IANA) allocates certain blocks of addresses to organizations. Individual users or small organizations can obtain their addresses either from the IANA or from an Internet service provider (ISP). You can visit the IANA homepage at www.iana.org. The IANA issues different class of IP addresses. There are five standard classes of IP addresses. They are:

Class A

Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range: 1.x.x.x to 126.x.x.x.

Class B

Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range: 128.1.x.x to 191.254.x.x.

Class C

Class C addresses may have up to 254 hosts in one network. Class C addresses use 24 bits for network addresses and eight bits for nodes. They range from 192.0.1x to 223.255.254.x.

Class D

Class D addresses are used for multicasts, in other word messages sent to multiple hosts. Class D addresses range from 224.0.0.0 to 239.255.255.255.

Class E

Class E addresses are for experimental purposes. For each unique value in the network portion of the address, the range base address (the host address contains only zeroes) is known as the network address and is not usually assigned to a host. The top address of the range (host address contains only ones) is unassigned. It is instead used as the broadcast address for sending a data packet to all hosts with the same network address simultaneously.

Netmask

The partition scheme that separates the different address classes is used to identify a netmask attached to the IP address. A netmask is a 32-bit quantity that, in logical combination (using an AND operator) with an IP address, forms the network address. The netmasks for Class A, B and C are for instance 255.0.0.0, 255.255.0.0 and 255.255.255.0.

The address 192.168.170.237 is a Class C IP address; its network portion is 192.168.170. Combining it with the Class C netmask using an AND operator as shown in this example leaves only the network portion of the address:

11000000 10101000 10101010 11101101 (192.168.170.237)

combined with:

11111111 11111111 11111111 00000000 (255.255.255.0)

resulting in:

11000000 10101000 10101010 00000000 (192.168.170.0)

An alternative to dotted decimal representation is to express the netmask as the quantity of ones from left to right. This number is added to the IP address after a slash (/) as '/n'. In this example, the address 192.168.170.237/24 could be written. This indicates that the netmask is 24 ones followed by eight zeroes.

Subnet Addressing

You can see that even with a Class C address, there are a large number of hosts per network. It would be a very inefficient use of the amount of IP addresses to supply every LAN with so many IP addresses. A smaller office LANs does not have that many devices. A more efficient technique is known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free.

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you only need to shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

Attention: The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

Freecom strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets
- When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.
- So that a local router or bridge recognizes which addresses are local and which are remote Private IP Addresses

If your local network is not connected to the Internet (for example, when using NAT), you can assign any IP addresses to your computers without problems. But to prevent problems and ease configuration, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

We recommend that you choose your private network number from this range. The DHCP server of the FSG is preconfigured to automatically assign private addresses.

For more information about address assignment, refer to RFC 1597, Address Allocation for Private Internets, and RFC 1466, Guidelines for Management of IP Address Space. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at www.ietf.org.

The IP address shortage

The Internet has grown larger than anyone ever imagined it could be. Although the exact size is unknown, the current estimate is that there are about 100 million hosts and more than 350 million users actively on the Internet. In fact, the rate of growth has been such that the Internet is effectively doubling in size each year.

When IP addressing first came out, everyone thought that there were plenty of addresses to cover any need. Theoretically, you could have 4,294,967,296 unique addresses. The actual number of available addresses is smaller (somewhere between 3.2 and 3.3 billion) because of the way that the addresses are separated into classes, and because some addresses are set aside for multicasting, testing or other special uses.

With the explosion of the Internet and the increase in home networks and business networks, the number of available IP addresses is simply not enough. The obvious solution is to redesign the address format to allow for more possible addresses. This is being developed (called IPv6), but will take many years to implement because it requires modification of the entire infrastructure of the Internet.

There are 2 systems in place now to help bring down the shortage of IP addresses.

DHCP

First, most users today have a dynamically given IP address or DHCP address from their provider. This means that the IP address given to you can change over time. This allows the provider to use the IP address for more then one person or device, since people are often online at different times. Optimal usage of IP addresses is guaranteed.

Your FSG gives its internal addresses to your computers in the same way. For the DNS (Domain Name System) it is difficult to translate your domain name "www.yourname.sharemydisk.com" to your IP address if your IP address keeps changing.

The system needs to be updated each time your IP address changes. Hence Dynamic DNS (DDNS) programs. These programs check the latest IP address and update the DNS system accordingly.

Multiple internal but only one external IP address

A second way to overcome this is to have a single device act on behalf of several other devices. Routers are typical examples. You have several PCs connect to the router, but only the router to the Internet. From an internet perspective, there is only one address. This scheme offers the additional benefit of simple firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

This works like a receptionist at a large office. Nobody knows your number; they all call the main number of the office and are then forwarded by the receptionist to you.

So how does the receptionist know what number to forward the call too? The caller tells the receptionist what name to look for and the receptionist has a listof names and numbers at her disposal so she can translate the name to the phone extension she needs.

On the Internet, it works exactly the same. NAT (RFC 1631) or Network Address Translation allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers.

Network Address Translation

When you visit a website via your computer, your router, or more specifically your NAT, remembers which computer on the internal network asked for the information. When the information (in this case the website you asked for) comes back, the router knows which computer on the internal network to send the information to. This is Network Address Translation or NAT.

Developed by Cisco, Network Address Translation is used by a device (firewall, router or computer) that sits between an internal network and the rest of the world. For more information about IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

Hosting a server

What If I want to host a server?

For others to be able to view your pictures on your computer, you need to run some type of service or server. A web server such as apache will allow others to securely watch the pictures or files on your site. But how does the NAT of your router know this time to which computer to forward the information?

Since the request comes from the internet, most routers are setup to disallow any traffic going into the internal network. (Firewall protection) In this case, since we want people to be able to see our pictures, we want the router to forward this information. We have to tell the router to do this.

Someone calling from the internet asks your router for a certain "port". This is the same as someone calling the receptionist and requesting a certain person by name. Ports are displayed as numbers but invariably map to pre described services. For instance, when someone requests a web page, they always ask for the service on port 80, the web server. Through NAT, it is possible to "map" a certain request for a service (a request for a port) to a certain PC on the internal network.

MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses. If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

Ethernet Cabling

There are two different types of cabling for Ethernet networks. Originally they used thick or thin coaxial cable, but most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. There are 2 types of RJ-45 cables available today, the Media Dependent Interface (MDI) cable and the Media Dependent Interface - Crossover (MDI-X) cable. The first cable is used to connect routers to PCs and the second to connect PCs directly to PCs. The sent and receive wires are switched from beginning to end in the crossover cables. Some Ethernet switch products, such as the FSG, are able to sense the polarity of a connection and automatically adapt to the proper cabling type.

Cable Quality

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or "Cat 5", by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

WARRANTY (valid in Europe/Turkey only):

We thank you for purchasing this Freecom product and hope you will enjoy using it.
In order to avoid unnecessary inconvenience on your part, we suggest reading the quick install guide, instruction manual and any additional electronic and or printed manuals. When problems occur we have a database with Frequently Asked Questions (FAQ) on our Freecom website (www.freecom.com), please check this site before you contact the helpdesk.

Your Guarantee
All Freecom products come with unlimited technical phone and web support. By this Guarantee, Freecom warrants their products to be free from defects in material and workmanship for a period listed below from the date of its original purchase. If during this period of guarantee the product proves defective due to improper materials or workmanship, Freecom will, without charge for labour or parts, at its sole discretion, repair or replace the product or its defective parts upon the terms and conditions set out below.

Conditions
This guarantee will be granted only when the original invoice or sales receipt (indicating the date of purchase, product and serial number) is presented together with the defective product and a Freecom RMA number received from the Freecom Website or given by a Freecom Service Center. Freecom reserves the right to refuse the free-of-charge guarantee services when the date of purchase of the product cannot be proven. This guarantee will not apply if the RMA number is missing, the serial number on the product has been altered, removed or made illegible.
This guarantee covers only the hardware components packaged with the product. This guarantee covers none of the following: (a) any consumable supplied with the product, such as media or batteries; (b) damage to or loss of any software programs, data or removable storage media; (c) any damage resulting from adaptations, changes or adjustments, which may have been made to the product, without the prior written consent of Freecom; (d) attempted repair by any party other than authorized by Freecom and (e) accidents, lightning, water, fire or any other such cause beyond the reasonable control of Freecom.

With respect to all services provided, Freecom is not responsible for any damage to or loss of any programs, data or other information stored on any media or any part of any product serviced. Freecom is not liable for the consequence of business loss in case of system failure. Be sure to exclude all parts not covered by this guarantee prior to returning the product to Freecom. Freecom is not liable for any loss or damage to these items. If during the repair of the product the contents of the hard drive are altered, deleted or in any way modified, Freecom is not liable whatsoever.

Repair parts and replacement products will be provided on an exchange basis and will be either new, equivalent to new or reconditioned. All replaced parts and products become the property of Freecom The period of guarantee for any product or part repaired or replaced in warranty shall be the balance of the original guarantee. Repairs or replacements on product or parts out of warranty carry **6 (six)** months guarantee.

All Freecom products come with unlimited free technical phone and web support.

Freecom Product	**Warranty period**
Classic & Internal Series	1 year (Two years in Europe)
FS & FX Series	1 year (Two years in Europe)
FHD Series	1 year (Two years in Europe)
FSG-xxx	1 year (Two years in Europe)
MediaPlayer-xxx	1 year (Two years in Europe)
DVB-T / USB Stick	1 year (Two years in Europe)
USB Floppy Disk Drive	1 year (Two years in Europe)
USBCard (Pro)	1 year (Two years in Europe)
USB 2.0 CardReader	1 year (Two years in Europe)
DAT & LTO Drives (retail)	3 years
DAT-S Kits	2 years